TRANSCRIPT OF PROCEEDINGS

IN THE MATTER OF:)
)
WORKSHOP, ENSURING BROADBAND)
RELIABILITY AND RESILIENCY)

Pages: 1 through 191

Place: Washington, D.C.

Date: September 8, 2011

BEFORE THE FEDERAL COMMUNICATIONS COMMISSION

HERITAGE REPORTING CORPORATION

Official Reporters
1220 L Street, N.W., Suite 600
Washington, D.C. 20005-4018
(202) 628-4888
contracts@hrccourtreporters.com

IN THE MATTER OF:)
)
WORKSHOP, ENSURING BROADBAND)
RELIABILITY AND RESILIENCY)

Room TWC-305
FCC Building
455 Twelfth Street, S.W.
Washington, D.C.

Thursday,
September 8, 2011

The parties met, pursuant to the notice, at 9:33 a.m.

BEFORE: JULIUS GENACHOWSKI,
Chairman

APPEARANCES:

For the Commission:

COMMISSIONER MICHAEL J. COPPS
COMMISSIONER MIGNON CLYBURN
COMMISSIONER ROBERT M. MCDOWELL

APPEARANCES: (Continuing)

Panel Moderators:

JEFFERY GOLDTHORP, ASSOCIATE CHIEF FOR CYBERSECURITY AND COMMUNICATIONS RELIABILITY, PUBLIC SAFETY AND HOMELAND SECURITY BUREAU (PSHSB), FCC

VERNON MOSLEY, SENIOR ENGINEER, CYBERSECURITY AND COMMUNICATIONS RELIABILITY DIVISION, PUBLIC SAFETY AND HOMELAND SECURITY BUREAU (PSHSB), FCC

Panel One, Benefits of Outage Reporting:

JOHN CARLSON, FINANCIAL SERVICES SECTOR COORDINATING COUNCIL
LAURIE FLAHERTY, NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION
MASARU FUJINO, EMBASSY OF JAPAN
STACY HARTMAN, CENTURYLINK
ROGER HIXSON, NATIONAL EMERGENCY NUMBER ASSOCIATION
COMMISSIONER ROBERT M. MCDOWELL, FCC

Panel Two, Metrics and Thresholds:

MARK ADAMS, COX ENTERPRISES, INCORPORATED
STACY HARTMAN, CENTURYLINK
ROBERT KONDILAS, COMPUTER SCIENCES CORPORATION
MICHAEL MAYERNIK, VONAGE
SCOTT ROBOHN, TELECOMMUNICATIONS INDUSTRY ASSOCIATION
MICHAEL ROWLEY, STATE OF NEW YORK DEPARTMENT OF PUBLIC SERVICE

Panel Three, Communications Reliability:

JOHN CARLSON, FINANCIAL SERVICES SECTOR COORDINATING COUNSEL
ANTHONY MYERS, MARYLAND PUBLIC SERVICE COMMISSION
SCOTT ROBOHN, TELECOMMUNICATIONS INDUSTRY ASSOCIATION
MICHAEL ROWLEY, STATE OF NEW YORK DEPARTMENT OF PUBLIC SERVICE
DUMINDA WIJESEKERA, PH.D., GEORGE MASON UNIVERSITY

P R O C E E D I N G S

(9:33 a.m.)

MR. GOLDTHORP: Good morning, and welcome to our workshop today on Ensuring Broadband Reliability and Resiliency. I appreciate you all coming out. This is being webcast as well, and my name is Jeff Goldthorp. I am the Associate Chief of Cybersecurity and Communications Reliability and Public Safety at the Homeland Security Bureau here at the FCC.

Let me just kick things off very quickly by turning it over to Jamie Barnett. Jamie is the Chief of the Public Safety and Homeland Security Bureau, and he will have a few opening remarks. Jamie.

(Applause.)

MR. BARNETT: Jeff, thank you so much, and thank you for your team, and the team from Public Safety at the Homeland Security Bureau, who put this together today.

For all of those who are joining us on the web, we appreciate you being here. For those of you who are here, I particularly thank you for coming through monsoon like weather. I think it is clear that if you made it here, you walk on water. You had to.

We welcome you to our Network Reliability

Workshop. I also would like to extend a very warm welcome to those who are panelists, and who have taken time out of their business schedules to share their expertise, their ideas, with us about these critical and timely issues, and I really think that we are in for a treat today as we consider these things together.

Henry Ford said that thinking is the hardest work there is, which is probably the reason why so few engage in it. The willingness of our panelists to think about some of these challenges presented by the ever changing communications landscape, and contribute their ideas, and their perspectives to these complex issues, I think really will improve the FCC's work, and the Nation's communications.

The President assigned the FCC the critical role of ensuring continuous operations and reconstitution of critical communications and services for the Nation's emergency preparedness and response efforts. That is a direct quote from the Presidential Directive.

This mission became starkly apparent within these past two weeks following the earthquake of August 23rd, and the chaos brought by Hurricane Irene up and down the coast.

We have much to do. We have done a lot in the past, but we still have much to learn, and to ensure that our Nation's communications infrastructure is reliable and resilient, and the FCC, along with all of the stakeholders, consistently put forth our best effort to continuously improve in the face of changing technology and crisis situations.

So, for example, during the earthquake and the tsunami in Japan, the country's broadband -- that country's broadband based warning systems enabled Japan's meteorological agency to issue alerts automatically via cell phones, and t.v. after the first less harmful earthquake, providing a short window -- you know, they give a p-wave right before it, and they are able to get that short window for people to prepare for the more powerful shockwave that followed.

Those with mobile phones were able to rely on their battery powered devices to access web-based disaster message boards, Twitter and social networking sites, to report on their status, and check for updates regarding their family and friends.

The capability to use wireless devices to access the internet was due in large part to the redundancy of Japan's wireless network, which can

automatically reroute signals over alternate paths if one route is destroyed or interrupted.

In the United States, we have no rules on redundancy, on backup power, and we have to ask whether that situation is acceptable, and whether that is the best way to be.

The migration of communications infrastructure from older technologies to broadband technology raises concerns about a communications network infrastructure that lacks time tested standards of the Legacy systems.

The Commission's reliability and resiliency proceeding is seeking input on exactly these issues. Another important effort by the Commission to ensure communications reliability is the Network Outage Reporting System, or NORS, which provides the Commission with essential information to enhance network security and reliability.

This mandatory reporting system provides data related to specific outages, which the Public Safety and Homeland Security Bureau uses to work with communications providers to improve their network reliability and resiliency.

We also develop aggregate reliability statistics based on NORS data, which we review with

the industry on a regular basis to facilitate industry-wide improvement in network reliability and resiliency.

Because of the NORS system, the Commission has a proven track record in taking vulnerabilities and reducing outages in circuit switched communications, with emphasis on the circuit switch.

While increasing numbers of consumers, businesses, and government agencies, rely on broadband, and interconnected voice services for every day and emergency communication needs, both voice and data, the Commission's outage reporting rules do not cover broadband ISPs or interconnected voice service providers.

The Smart Grid relies on broadband communications. Telemedicine relies on broadband. The Federal Reserve's Fedwire, the IP based funds and security transfer network that services financial institutions, carries over a half-million transactions per day, worth $3.7 trillion per day.

Yet, to the extent that significant outages occur on these networks, the Commission currently has no way of monitoring the reliability and availability of these systems.

To address this deficiency the Commission

has proposed to expand its outage rules to interconnected voice providers, and broadband ISPs. The broadband communications infrastructure constitutes a large and growing share of our critical communications infrastructure.

Yet, outages in broadband networks are not uncommon. Ensuring the reliability of those networks has become vital to the public interest. Another timely example of the Commission's efforts to ensure communications resilience during disaster times is our Voluntary Disaster Information Reporting System, or VDIRS, through which the Commission collects operational status and restoration information from communications providers, including wireless, wireline broadcast cable providers, all this during major disasters and subsequent to recovery efforts.

VDIRS gives communication providers a single coordinated, consistent, and voluntary Federal process to report their communications infrastructure status information during those times of crisis.

This system proved critical during the recent communication to outages suffered from Hurricane Irene. So, believe it or not, this particular workshop was planned long before the earthquake, long before the hurricane, and long before

the monsoon that we are having right now.

But I think that you can see that there is a certain urgency to it, a certain relevancy, and we hope today that we will be able to come up with some great discussions and some great answers before the next unexpected, and yet inevitable, event.

So thank you very much for being here. So, I have the honor of introducing Commissioner McDowell. One of the things that I think that will be apparent to you today is that the emphasis with which our Commissioners place on this particular subject matter today, I think that you are going to get to see the whole Commission today at one point or another.

Commissioner McDowell, we greatly appreciate you being here, and I would turn the floor over to you. Thank you for any comments that you have for us, sir.

COMMISSIONER MCDOWELL: I thought I was going to be late, too, as we all navigated the waters coming down from the heavens. I think that we all need to build an ark here, and we are very well equipped here at the FCC, because we have an Admiral right here in our ranks. So we have someone to captain that ark. That's right, Admiral Noah.

And with all the words being said in

Washington this week, there is one word that you will not hear. Sunscreen. You just don't need it during a week like this. It is dark pretty much 24-7 this week.

So thank you so much to the Admiral, and to everyone in the Bureau for putting this together. Not only are you an Admiral, but you are a clairvoyant, because this is incredibly well timed, this workshop. I think we are going to learn a lot today.

I am going to keep my remarks very brief. I want to thank all of our panelists who are going to come and tell us their views and what they have learned all the way through probably even today about how events can affect the reliability of our networks and our public safety.

And I do especially want to extend a special warm welcome to our guest from the government of Japan, and to thank them for imparting upon us what they have learned from their recent tragedies as well. So, welcome.

So public safety and homeland security are always a priority for the FCC, but this recent one, two -- and now three -- punch of an earthquake, hurricane, and monsoon, hitting the East Coast, our most densely populated area of our country, has

heightened awareness that we need to reexamine what we are doing in this area.

It is important to constantly reevaluate and learn from what is happening. These events, of course, coupled with the 10th anniversary of the 9/11 attacks, make it a perfect time to analyze what we are doing right, and what we need to improve.

I think that the Bureau's and the Chairman's office deserve a high degree of kudos for working in real-time, and keeping us all informed of what has been going on, and really just pouncing on the opportunity to learn more, and to make sure that the public, that the consumers throughout the country, are being served in the best possible way when it comes to communications infrastructure.

One area that is related, but not exactly on point for what we are going to talk about in the workshop today, but I want to thank the Bureau for looking into it even before I asked them to, is something that I experienced, and I think that Commissioner Clyburn also experienced during earthquake.

We were in Aspen together for a conference, and we were on a panel together, and just a few minutes before the panels when the earthquake hit. So

I immediately called to find out what the extent of the damage was, and found that I could not get through to my team, who were using wireless phones.

And so I used the wireless priority service. Some government officials get this card, which gives us a little code that we can dial to get through in times of extreme congestion.

And it ends up after doing an initial investigation that still today, even 10 years after 9/11, where there is a spike in congestion around a specific area with wireless users, you still can't get through even with a WPS.

And that is something that we need to examine, learn from, and improve. I want to flag that issue, and I do appreciate the Commission and the Bureau for looking into this right now, and I look forward to learning what we find out, and what we can do to improve it as quickly as possible, because that was a big concern on 9/11, is that first of all everyone should be able to use their wireless device in times of a crisis.

But especially those that are involved with first response, or with making sure that the infrastructure is intact, or can be salvaged if there is a problem.

And so that is why some of us get these cards, is to try to be able to get through in the most critical way, and if it didn't work, we need to find out why it didn't work, and what can we do in the future to make sure that it does work.

So, thank you all very much. I promised that I would keep my remarks short, and hopefully we can all stay dry here in this room so that we don't grow mold otherwise.

But in any case, I look forward to learning more from what we have here today, and throughout the whole process. Thank you.

(Applause.)

MR. GOLDTHORP: Thank you, and as the Commissioner said, we do have some folks here from the international community that will be speaking to us and sharing their ideas, and I want to first thank the coordination with the International Bureau, which helped make this first presentation possible, and the other visitor from Japan as well. That was very helpful and we appreciate that.

We are going to lead off today with some remarks by Mr. Uffe Jensen, and let me just say a few things to introduce you to him. Mr. Jensen began his career in the Danish Department of Taxation in 1993.

He moved to the European Commission Anti-Fraud Office in Brussels, dealing primarily with financial interests. He has also worked in the Reform of Custom Services in the countries of the former Soviet Union, as coordinator of International IT development for the Director General for Taxation.

And on the personal staff of Danish EU Commissioner Nielson, and with the EU delegation in Yerevan, Armenia. Since May of this year, Mr. Jensen has served in the EU delegation to the United States in Washington, D.C.

He covers the EU-U.S. cooperation in a number of areas related to justice and home affairs. In addition to a civil service education in customs and taxation, Mr. Jensen holds a Bachelors in -- or rather a Masters in Public Administration, a post-graduate Masters in International Politics, and a degree Social Science.

So, please join me in welcoming Mr. Jensen to the podium, and we are looking forward to hearing what you have to share with us today.

(Applause.)

MR. JENSEN: Good morning everybody, and thank you, Jeff, for this introduction. Sometimes I have the privilege to be the one-eyed king in the

kingdom of the blind, and despite the fact that the introduction sounds good to me, I think it proves that today that I am the blind together with all those who can see and have knowledge on these issues.

Nevertheless, I hope that I can give you some kind of overview about the thinkings behind the developments in the European Union, and what led to the legislation that we have on these issues.

And I have to apologize for the slides. They are very legalistic, and they are referring to legal texts, and you might not be able to see all the details. I have heard that the slides will be made available to everybody after this presentation.

The 2009 Telecoms Reform introduced the notion of security breaches and reporting obligations at the European Union level. So this is a novelty from 2009, and at that time, prior to this one, we only had two Member States.

You know, the European Union consists of 27 Member States currently, and only two Member States had experience with this kind of reporting mechanism, and these Member States were Finland and Sweden.

And I will come a little bit into that more if people have questions, and let me try to answer those ones, but the experience gained by Sweden and

Finland has formed part of the baseline for the further developments of the directive.

I also have to say that the experience gained by the U.S. has also played a major role because the American system was before us when it came to regulations for mandatory disclosure of security incidents involving personal identifiable information.

And this is kind of a sensitive issue for Europeans when it comes to privacy issues. You can see that there is a reference to the E-Privacy Directive here.

I just put it in because this is very important, and is one of the important elements that has led to these obligations to the providers, and it is something that is very sensitive as I said to the European Parliament and the European decision makers.

The amendment of Directive 2002 on a common regulatory framework, as I said, it has a new chapter in 2009. The 2002 regulation was amended in 2009 to include security issues, which was not the case before.

I have to say that the leading up to these changes was caused by a lot of issues, especially the fact that we now realize that security breaches are not something which is only on a national level. It

is also something which is transnational, and the European Union, as you know, has 27 different Member States.

The whole telecom reform was also triggered back in 2002, and also the amendment in 2009 was triggered by an overall political development tin the European Union, whereby we had one of the key functions of the European Union, which is what we call the internal market, where competition should be free in the markets.

And there was some debilitation faults on telecommunications, and energy markets had been liberalized, and that means that we also need to make sure that there is a uniform European framework legislation in place.

I don't want to go into too many legalistic details, but I think for the sake of clarity that I have to just very briefly say that there is basically two kinds of European legislation.

We have regulations, which are EU regulations, which are correctly binding on the EU Member States. So if the European Union, by the European Commission, and the Parliament, and the Council, decides a new legislation, and we call it a regulation, that means that the Member States have to

implement that regulation according to the text, every word of the text.

Whereas, in this case, we are talking about a directive. A directive is a framework legislation, which means that the European Union Member States individually can amend national legislation, but they have to fulfill the objectives of the legislation.

This is a little bit important in this case since there is a difference from the regulations, insofar as if you have a regulation, there is more access to power on the European level. In this case, the enforcement of a directive is only by the European Member States.

The European Commission does not have an enforcement role. Our Agency, ENISA, is also set up as a kind of a body, which is the Center of Excellency, which is trying to communicate best practices, but not having an enforcement role. The enforcement lies with the Member States also in this case.

What are we talking about here? We are talking about the amendment to this old directive, the directive of 2002, which was amended in 2009, and here Article 13 established the reporting mechanism that we are talking about.

And we say that the Member States shall ensure that undertakings of providing public communication networks are properly available, and electronic communication services will notify the competent national authority of any breaches of security or loss of integrity that has a significant impact on the operation of networks and services.

So basically we are talking about breaches of security, loss of integrity, and we talk about significant impact, however that is defined, and we talk about networks, and we talk about services, and we talk about telecom undertakings who are providing public communication networks, or publicly available electronic communication services.

When we are talking about the undertakings of the providers here, there is another issue, which is perhaps useful for you to know that we are talking about those companies who normally would have a license by one of the Member States to make these services available for the public.

So there is a contract in any case between the service provider and the particular Member States, and this is what we are talking about here. We are talking a little bit about old fashioned telecommunications, and that has of course developed

rapidly over the years.

So now we have other services, and just having the networks available as well. It is difficult to see because of the text there, but we are talking about a risk management context here. So, Article 30(a)(1) and (2) actually say that Member States shall ensure that undertakings providing public communication networks, and communication services, that they take the appropriate technical and organizational missions to appropriately manage the risk posed to security of networks and services.

And here we are having some language with regard to the state-of-the-art. These measures shall ensure a level of security appropriate to the risk presented.

So we are talking about reporting of security breaches linked to risk management, and I have to say that if we are discussing the impact on companies affected by this one, I would say that there is nothing in the reporting system that we are trying to develop that should not already be in place in that particular company.

I mean, the company should have an internal reporting mechanism and that they should know this kind of breaches already, and so it is only a matter

of making it obligatory to report these breaches to the national authorities.

What we are talking about is three types of reporting on the European level. So we have the first reporting from the undertakings from the companies to the competent national regulatory authorities. That is the starting point.

And here since I started to say today, we are talking about a directive. So the national Member States, they have the possibility to enforce, to ask for stricter legislation than the European legislation.

So there is a matter of how the national authorities ask their companies to report to them, and so we are talking about minimum level reporting in the European Union, but there might be more strict reporting requirements from the companies to the national authorities.

We also have a reporting obligation imposed on the national regulatory authorities because they have to report to other Member States in case of emergencies, and in cases of significance, and they might have to also inform the public of these kinds of security breaches that we are talking about.

And then finally the said reporting which we

are trying to develop for the time being is the reporting for the national regulatory authorities to ENISA, our agency, and to the European Commission.

There is another complication in the European system. We do have many complications in our systems, but one of them is, of course, that having 27 Member States who are sovereign Member States, means that they alone have the right to define how they are managing their regulatory's setup, which are the authorities who are involved, I guess, in the American context.

And so you also have a lot of agencies involved in various items, and here in the European Union,k it is for the Member States to define which is the authority for what kind of incidents. It is not something that the European Union is imposing.

The next slide is a bit about the timing, and about the implementation. In the legislation that we put in on the 25th of May for the transportation data of the telecom package, and by the 25th of May, the Member States would have to introduce the directive into national legislation.

Since as I said at the beginning that it was only Finland and Sweden who had experience with this one, actually the state of play of a lot of Member

States did not develop the concept further, and did not make much more complicated legislation, but simply used the text which we had, which is kind of a broad text.

Then we also have the European Commission, which is kind of the executive body of the European Union, might also take up technical implementing measures, with a view to harmonizing the national measures concerning reporting.

And here I have to say again that it has been very important for the European Union not to impose legislation on the Member States, the companies, and so it has been a kind of the whole discussions during work groups, and has been in a way that we are trying to elaborate a common baseline in cooperation with the Member States.

And the Member States themselves will have had a lot of concentration normally with those companies who are going to be affected. The technical guidelines that we are going to finalize in September or October of this year, and we would happily share them with you as soon as they are finalized.

And we will send them to Greg and to Jeff as soon as we have them. They are as I said going to be finalized now, and as I said, they are bottom up

approaches that we are talking about. They are guidelines.

And there is a very strong demand for Member States to comply with these guidelines that we are going to agree on, but legally speaking, they are to be considered guidelines, and then we will see how that actually materialize itself when we get the first reporting from the Member States.

We will then know much more about whether we made the guidelines in the correct way, and whether we made all the definitions of the various things to report on, and whether they are logical, because I think only practical experience will show whether we are on the right track.

But the whole idea is that in any case that the reporting from the companies to the national regulatory authorities, from the national level to the European level, the idea is that it is kind of a learning process all the time.

So we want to have a kind of service with that, and the experience gained will be used, and evaluated upon, and made available for best practices in any instance.

This one will be very short, and just to say that the work on the technical guidelines is in

progress, and it is important that the slides, when you see the slides which follow, goes a little bit more into what we have foreseen for reporting.

In practical terms, they should not be considered too definitive. They are under elaboration and as I said, again the experience gained in the future will mean that we might have to amend them again.

So the content of the reporting scheme, I guess, is where you might be able to extract in the future some of our knowledge, and we definitely need your knowledge as well.

But here we have kind of an overview about what are we going to ask for. So we are going to on the European level ask for annual aggregated and numerous reports of all reported security breaches, and here without the name of the provider.

Personally, I don't know whether it is possible or not to know who is the provider because I guess it is a small community of big companies that we are talking about. But anyway we are not going to name them, but we are going to use it as a constructive tool to distribute knowledge.

So basically the things that we have, the four things so far, for describing the basis, is the

date of occurrence, and it is the date of detection, and it is the affected assets and services, and it is information on the root cause, including some kind of trend indicators, and what are the vulnerabilities that would need to be explored.

We also want to know a bit about the impact. We want to know how these breaches have been handled, and what is the response approach by the Member States, and perhaps also by the companies.

And finally we want to know what are the initiatives taken to avoid similar breaches in the future. So coming back to my initial remarks about my own blindness in this one, this is a more complicated slide for me, because it has a very simple list of assets and services affected, but for me, it is a bit difficult to see exactly where there is the limit between various services.

But definitely we are talking about telephone voice-fixed networks, and we are talking about data services, satellite communications, and fixed networks, and wireless broadcast services.

And telephone voice would be domestic telecommunication networks. That is what we are talking about here. So we are talking about a key telephone system, private branch exchange trunks, and

various data arrangements.

And we are also talking about networks that support digital communications for voice and internet data services on cell phone networks. So that is at least the ambition for the time being.

When we talk about data, we are talking about services which comprise non-audio primary service components, and eventually additional secondary service components.

So we are talking about internet connections when people are using the internet for communication purposes, and these can be operated by the governments, and they can be operated by industrial, academia, private parties.

And we are also talking about e-mail services, and that is also important. Satellite communications, that is all communications between earth stations and satellite positions.

Violet broadcast services. That is a radio communication service in which the transmissions are intended for direct reception by the general public, and this service mode includes sound transmissions, television transmissions even, and other types of transmissions.

The technical aspects also includes some

parameters that they are trying to set. So I said I will need to know the amount of uses affected, and the duration of the breach, and the geographical spread, and even down to at the regional level.

And then an important issue, of course, when we talk about public communication networks is the impact on the emergency services. You have the 911 here, and we have 112.

So we will see how badly that would be affected by this breach, and basically what we are talking about -- we are not only talking about in this case usual security breaches. We are talking about the dysfunctioning of public services in the internal market. So there is overlapping interest to get these services to function.

And I shortly mentioned the thresholds that we have put into the guidelines. They are minimum. I mean, these ones, we don't discuss with Member States. Some might argue that the limits could have been set differently, and they might not be logically developed.

But I think the graphic illustration looks nice at least, and that we have a very logical framework that we have outlined. The Member States can if they want, and if they feel the need for it,

they can make stricter reporting thresholds.

So it might be a bit difficult for you to see, but the threshold suggested is on the top level, you see from one hour to two hours, and two to four hours, and four hours to six, and six to eight, and more than eight hours security or unavailability for one reason or another.

And then we have on the vertical line, you have the amount of uses affected. So there is a combination of uses affected and the time frame. And as we said in this one, it does not necessarily mean that significance is only linked to numbers.

I mean, you can have significant security breaches, whether on time, and based on the type of breach, it can be also breaches on the non-integrity of the data held by the providers, which will make in my view an obligation to the companies to report to the Member States.

Of course, a breach can be significant, and important for a number of reasons outside of this particular table, but at least we have a minimum threshold level for reporting.

This slide is showing the objectives of collecting data on security breaches, and it is to get better access and dissemination of information among

the interested parties.

It is also linked to information that is important for the risk management for all of our interested parties, and it is about a learning process for policymakers and providers.

I think that there are many more reasons for having a reporting system, and as I said up front, my experience with providers of IT services is that the professional providers will have these kind of information available.

Jeff told you that I used to work in the European Union Customs Office, where we did -- where we had some very, very big computer systems, and if they broke down, the entire import-export operations, and the transient operations of the European Union would go down.

So we had 24 hour, every minute, monitoring of about the availability of breaches, et cetera. So I don't think that it is an impossible burden to put on those who are having these licenses to telecommunication services.

And I think that it is in everybody's interests when there is a breach of security to know what the reason is, and how can we deal with that one, and these information are going to be disseminated.

There is another issue also. I mentioned at the beginning that there was many reasons for the amendment of the legislation. One of them is linked to the competitiveness of the European market when we in 2000, the European Union made what we called the Lisbon Strategy, which was caused by the fact that at that time the European Union was less competitive than Japan and the United States.

So we had to do something, and we made liberalization of the emery markets, and telecommunications, et cetera, and we enhanced the competitiveness.

And to have -- it is important to have some kind of transparency. It is important to have some kind of minimum standards also when it comes to security to ensure that what we wanted to achieve was to be the most competitive knowledge-based economy by 2010, and I am afraid that we really didn't reach that goal.

But at least when you are talking about a competitive market, we need to be sure that the telecom services are reliable, and are available. So we need to have a set of minimum standards for the Member States. And it goes into the overall competitiveness of the European Union as well.

As I said at the beginning the European Commission is very pleased that we are invited to this workshop, and I apologize that the experts from headquarters were not available to come today.

I had promised to take back all the questions that you have if I can't answer them. I have also promised that when they, I will try to facilitate contacts between you and my colleagues back in Brussels, and they are really, really keen learning from the American experience in this field.

And here you have some useful contacts as well with my colleagues back home, and the colleagues in the agency who is dealing with this one. Thank you very much.

(Applause.)

MR. BARNETT: Mr. Jensen, thank you so much for these key insights to the European approaches as to this, and as to the depth and breathe of our discussion. I appreciate your presence here today.

Now it is my pleasure to introduce our own FCC Commissioner, Mignon Clyburn, who takes a special interest in this for a couple of reasons. One is that she hails from a State that is continually a buffer-bumper for hurricanes and other weather like, and they were in fact affected this time as well.

And then she also served many years with the South Carolina Public Utilities Commission. So I think that has added to her passion for this particular subject. Thank you so much for spending time with her, and please welcome Commissioner Clyburn.

(Applause.)

COMMISSIONER CLYBURN: Good morning everyone. As Admiral Barnett affirmed, I am from South Carolina, a beautiful State, but a State that is quite vulnerable, and so you are absolutely right. These issues mean a lot to me.

It explains probably a lot about my demeanor, too. We grow up a little tough, but we are resilient. Again, I would like to thank you for inviting me here this morning, and want to take a moment to comment you and your staff at the Public Safety and Homeland Security Bureau for organizing this terrific agenda.

When Admiral Barnett briefed the Commission about the FCC's emergency response efforts in Haiti, he highlighted the value of teamwork from all of our partners.

To be best prepared for natural disasters, we need collaboration from the widest array of

stakeholders, for such collaboration allows us to fashion solutions that will achieve important policy initiatives without imposing unreasonable burdens on communications companies.

The emergency response efforts in Haiti and Japan taught us another lesson, however. They showed how vital broadband networks are to rescue efforts during large scale disasters.

We know that relief workers in Haiti and Japan developed several new broadband applications which allowed them to find people and deliver urgent medical care and aid.

That experience teaches me that we must take appropriate steps to ensure the continuity and reliability not just of Legacy networks, but of broadband networks as well.

The impressive list of participants on this agenda this morning affirms that the staff at the bureau has worked hard to attract a wide range of ideas on the best ways to ensure the continuity and reliability of Legacy and broadband networks.

At FCC workshops, we expect to hear important contributions from service providers, as well as State and Federal officials. We are not, however, often graced with the presence of consular

from the Japanese Embassy, or European Commission. We are happy about your inclusion this morning.

In light of the disasters and tremendous rescue efforts in Haiti, Chile, and Japan, there is much we can learn from our international partners and friends.

So I again welcome all of our guests to the Commission, and look forward to hearing your recommendations.

(Applause.)

MR. GOLDTHORP: Thank you, Commissioner, and I would like to invite our panelists for the first panel to take the dias now. And I realized late in the game that I didn't get wired up for a wireless mike, and we are going to fix that in a moment without interrupting the flow, because I hate talking from a podium.

(Pause.)

MR. GOLDTHORP: And the way that we will get started is once the panels gets seated, we will just do very brief introductions. The panelists will introduce themselves, their name, and where they work, and their role.

There won't be prepared remarks. It was all set up that way. And then when we are done, our

visitor from Japan will have some extra time -- about 10 minutes -- to talk about how things are done in Japan, and then we will roll into the usual format. So why don't we begin, John, with you, and if you want to say a few words by way of introduction.

MR. CARLSON: Okay. Great. Good morning. Thank you, Jeff, very much for including me today. My name is John Carlson, and I represent the Financial Services Sector Coordinating Council, which is made up of 52 associations and large financial institutions that is focused on resiliency of the telecommunications networks as it relates to the financial services sector.

Our sector has had a lot of experience with our dependence on telecom. It is core to our business. We know that we are dependent. We have had a number of experiences in which we have seen that dependency. 9/11 was certainly one of them, in terms of the lack of resiliency and diversity in some of the circuits that we relied upon.

And our sector, which is made up of the critical infrastructure, has worked over the past decade since 9/11 to really focus on the need for enhanced resiliency, both in terms of what we can do as major buyers of technology services, including

telecom services, but also enhanced information sharing and best practices that we can generate as a sector.

One of the messages that I want to convey today is that we think that it is very important to make sure that financial institutions and other consumers have the information that they need in order to make wise decisions.

And network outage reporting is one of those metrics that could be very useful to be a good buyer of service, and also to ensure that we have the level of resiliency that we need in our networks.

It is of particular concern to financial services, because we are heavily regulated. We have requirements in terms of the ability to recover services within hours, depending on what type of operation you are involved in.

Many of these requirements were an outgrowth of the 9/11 response, and the actions that the Federal regulators, the Federal Reserve, the OCC, the Securities and Exchange Commission, took in order to enhance resiliency.

So we need the tools to make those good decisions, and we know that technology is constantly evolving. Broadband obviously was an emerging

technology a few years ago.

It is now a Legacy technology, and so we need those same kind of tools and information in order to be good purchasers of technology services.

MR. GOLDTHORP: Thank you, John. Laurie.

MS. FLAHERTY: Good morning. Thank you so much for inviting me to participate this morning. My name is Laurie Flaherty, and I the Coordinator for the National 9/11 Program, which is housed within the National Highway Traffic Safety administration of the Department of Transportation.

We have three responsibilities in that program. One is to improve and increase the amount of collaboration among all of the stakeholders involved in providing 911 services.

We also have a clearinghouse to provide information specifically on 911 technology and operations, and we also administer our grant program, which is for the 911 public safety answering points.

In short, our job is to get 911 to the table every chance that we get, and to connect the dots between all of the players every chance that we get. I think the reason for our participation here is obvious, and so I will stop there, and thank you very much.

MR. GOLDTHORP: Thanks, Laurie. Roger.

MR. HIXSON: My name is Roger Hixson, and I am the Technical Issues Director at the National Emergency Number Association. We are also concerned with our counterparts in the European Union, which is the European Emergency Number Association.

So we are keeping track of not only what goes on here in North America, but also in the European Union as well.

Our primary activity right now is the development of standards and procedures for Next Generation 911, which is the replacement eventually for what we have today as an enhanced 911 system.

In both today's system and services for 911, as well as the future that is developing week by week, and month by month at this point, the dependency or dependability of IP networks, both public and privately managed IP networks, that are used for the 911 system, as compared to analog networks use 391 today, and in all of those cases, we are very concerned about dependability, and reliability, duplication, redundancy, et cetera, for the networks upon which these public service systems operate and run.

As well as the same conditions or qualities

for the reasoning service provider environment that calls come through to 911 for emergency requests for assistance, and also the delivery mechanism, or networks, that take those calls to the public safety answering points and other emergency services entities.

So we have a long history of being concerned about these kinds of topics, and how we deal with outages, and the measuring of outage conditions. I guess that's all that I need to say. Thank you.

MR. GOLDTHORP: Thank you, Roger. Stacy.

MS. HARTMAN: Good morning. I am Stacy Hartman with CenturyLink. I will start by thanking you for the opportunity to be here today. CenturyLink certainly takes our collaborative efforts with the FCC very seriously, and we have a long history of working with the FCC and the industry in the realm of outage reporting reliability and resiliency, and network management in general.

I am here today obviously to bring the service provider's perspective to outage reporting, and I am looking forward to the opportunity to discuss a little bit more in detail and collaborate as we move forward.

MR. GOLDTHORP: Mr. Fujino.

MR. FUJINO: Good morning. My name is Masaru Fujino, and thank you for inviting me to participate here today. I have been working for the Embassy of Japan for three years, and before that, I was working for the Ministry of Affairs and Communications entity, and I was on the staff, and Reliability and resiliency is a very important issue in Japan too. Thank you very much.

MR. GOLDTHORP: Okay. Would you like to take a moment now to tell us a little bit about what's happening in Japan, and then we'll just roll into the panel.

MR. FUJINO: In Japan, they're having both a mandatory outage reporting and a preemptory reporting made by communication providers to the Ministry of Affairs and Communications, and reflecting the increase of IP-based communications, the range of mandatory reporting was expanded in 2008. I will talk about this later.

There are two types of mandatory reports. They are immediate reports, and quarterly reports. Both are required for all kinds of communication providers, including those involved in traditional fixed telephone, and cell phones, and internet access, voice, and others.

There are some exceptions for the reporting requirements, but they do not have to report on minor accidents, or additional services, like co-rating services.

Both of the immediate reports and the quarterly reports mandate for the suspension of service and repair of the quality of service that is caused by certain kinds of accidents.

When we say the suspension of service, complete suspension of the service is included, of course, and suspension of either transmission or reception alone is included as well.

And for impaired quality, there are some criteria. For example, if loss of voice transmission is higher than 80 percent, that can be impaired quality to be reported.

Or if a delay of e-mail is longer than one day within the coverage of the same provider that provides the network. It can impair the quality, too. We define several types of accidents and that require immediate reports, or quarterly reports, depending on which type of an accident occurred.

If a severe accident defined in the Ministry of Ordinance of MIC occurs, communication service providers have to do an immediate report. That means

that they have to report the outlines of the accident immediately after the severe accident, and then in more detail within 30 days after the accident.

A severe accident which needs an immediate report is an accident caused by a malfunction of communication facilities like transmission lines or a switch, and affected 30,000 customers or more for two hours or longer.

If the malfunction occurred at important transmission facilities, like satellite or submarine cable, the provider establishes that they have to then report if it has without communications for two hours or longer, no matter how many customers are affected.

And if an accident affected 30 thousand customers or more, but just for a short period, or it occurred for two hours or longer, but affected just a small number of customers, they don't need to do an immediate report but have to do a quarterly report instead.

They have to report to the MIC within a period not exceeding two months after every quarter. In that case, they have to report even if it is not a matter of telecommunication facilities but some other facilities, like systems for making contacts with customers.

In Fiscal Year 2010, there were 15 immediate reports in one year, while there were more than 48 thousand quarterly reports made in the same fiscal year.

There have been two major changes which were enacted in 2008 affecting the rapid increase of IP based communications, including VoIP. We counted 26 million VoIP users in March of 2011, and where the number of traditional fixed phone service subscribers was 40 million at the same time.

And 18 million users out of 26 million VoIP users, there are more than two-thirds for VoIP users that are using high quality VoIP, which are required to have an emergency call function, or something equivalent to the American 911.

The number of VoIP users, and the high quality VoIP users with an emergency call function are increasing, while the number of users of a VoIP without an emergency call function requirement is decreasing in Japan.

So what we are facing is an increasing dependency on VoIP and internet access as a communication tool and as a way for emergency calls. We modified the mandatory outage reporting system in two ways affecting that trend in 2007, and enacted in

2008.

One of the two was the introduction of our reporting for impairment of quality of services. Before then only the suspension of service was considered as an outage that was reported to MIC.

Impaired quality of a service was added because they found out that there are many delays, rather than suspended service in IP based services, but if it is constantly in delay, you do not understand anything when you hear from the emergency -- you know, from VoIP. That is why.

And the other modification enacted in 2008 was the introduction of a quarterly report for relatively minor accidents. The introduction was done because they saw that there were many minor accidents which leads to a severe accident.

We see the number of accidents is increasing as IP based services are getting popular. In Fiscal Year 2003, there were just seven severe accidents in one year, but in Fiscal Year 2009, the number reached to 18. We found many accidents on IP based networks from, for example, their foundering and their software malfunction, which are relatively few for traditional telephone networks. So now we get information on minor accidents from a quarterly report, and we

publish data every six months for information sharing.

There have been voluntary reporting, too. The most notable one is reporting using what is called an emergency information gathering network, operated by MIC for daily reports from major providers like NTT, KDDIs, Softbank, after major disasters.

The program can input the data from anywhere on the internet from MIC. The MIC makes the outcomes publicly available daily. We use kind of a unified format for the system, and the system services are quite simple, but the MIC and those major carriers are doing the training for the operation of the system quarterly.

This year, daily reports have been made after the heavy snow in January, and after the eruption of Mount Kirishima in February, and after the great East Japan earthquake on March 11th.

Because of these reportings after the earthquake, MIC couldn't know that outage of broadband and telephone service was rather spreading a few days after the earthquake.

We found that because the commercial electricity shortage was long, and providers' batteries were becoming drained, the backup generators were running out of fuel.

Because of that, MIC could ask another agency, the Agency for Natural Resources and Energy, through the Prime Minister's office, to supply fuel to the service providers for the providers' own generators, and that supply was realized successfully.

That was the outline of the mandatory report and the quarterly report. MIC gathered essential information by mandatory reports, and a daily report is realized on the basis of the mandatory reports.

I have to admit that the management report but not be overall or as precise as a mandatory report, but we can have an overview on the trend of outages after disasters.

Now, let me tell you why these kinds of reports are very important. There are two merits. First, with reported information, the government can take an appropriate action when necessary. I will give you an example of an improvement made from the reports.

In 2008, when major carriers, such as Softbank Mobile, reported to MIC several severe accidents on transmissions for mobile phone equipment, the accident made outages on IP communications affecting 700 thousand customers.

From the reports from Softbank Mobile, MIC

found out that backup facilities were not working after the accidents. MIC asked Softbank to take appropriate measures to fix them immediately on May 14th.

And Softbank did measures in responding to MIC's action. That was one example of the actual improvement made from the reports. The second merit of the report is that communication providers can share information that the government makes public.

MIC publishes statistics of outages, including data on each facilities that are damaged, and why accidents happen, twice a year. Every six months. That should be helpful for the providers to take measures against future possible accidents.

The data has already shown us that while the number of accidents caused by human mistake is not increasing, but those caused by software malfunction, or by thunder, are increasing with the spread of IP networks.

The providers could not share those kind of data with the United States without MIC's publication, but because of the reported information, they now share those valuable data and analysis.

While they have benefits, the model reporting is not very costly. They often do the

immediate reports by a phone call, or e-mail, in Japan. And they can use very simplified formats for the quarterly reports.

MR. GOLDTHORP: Mr. Fujino, if you want to make a few remarks just to wind things down, and we can get on with the panel. Thank you.

MR. FUJINO: Well, for that merit, we have made those kinds of -- you know, both management reporting and outage reports. Thank you very much.

MR. GOLDTHORP: Thank you, and thank you for coming, and I want to thank all the panelists for coming today, and being part of the workshop and this panel.

We have heard from Mr. Fujino from Japan, and we have heard from Mr. Jensen from the other side of the world about how things are done in different countries.

All of you are familiar at least in one form or another with how we do these kinds of things here, and I will do a five floor elevator talk on how we do it here, and then we will jump in and talk about how we have done it here, and how we are proposing to change it, and get your ideas on that.

So, the five floor talk is what we do is a combination of voluntary best practices and rules for

reporting that you are all familiar with, and we have done the rules for reporting certainly for the last seven years, six or seven years, and longer than that really, but we have gotten a lot more data in the last six or seven years.

I think that it is true that in all of our interactions with communications providers that we are not putting ourselves in the position of telling carriers or communications providers how to run their business.

We don't have rules on what best practices people should do, but we do have rules that require a certain degree of transparency about how communications networks are performing from a reliability perspective, and we use that data to work with carriers, and others, to improve service reliability for emergency services, for other services, for consumers, or critical services.

So let me ask you -- and in your opening remarks, a lot of you were talking about how vital communications have been to you, and so starting first with what I call Legacy.

And I think it was you, John, who said, well, broadband is the new Legacy, and I think that there is true in that. But thinking back to what we

customarily call Legacy communication services, and the services over which we have rules today for reporting, to what extent and how do you rely on those services today?

If you want to add anything to whatever you have already said, and then we will talk about how our rules fit into that. So, John, do you want to start?

MR. CARLSON: Sure. I think we can probably start with the outages, and you can't manage what you can't measure, and that becomes very important in the financial services industry, and that's why some of the outage reporting becomes very helpful as a took for understanding, and to compare different providers, in terms of the service that they deliver.

I think that some of our experiences in the financial services industry, because we are big proponents of best practices, and I have worked on numerous best practices.

My previous organization was actually involved in MBREC, the predecessor to CSRIC, along with the Federal Reserve Board of Governors, and we think that there is a lot of value in doing this best practices work.

I think sometimes you run up against these points where the best practices can only go so far,

and sometimes you do need some of those bright lines to say that these are requirements, and these are thing that we need to have in order to make this system work as efficiently as possible, and to really let the marketplace be as efficient as possible.

So I think that one of the key concerns that we have had is that we need the information in order to be good consumers, and evaluate, and also to have some sort of baseline resiliency levels in order to provide the services that we are in the business to provide.

And frankly are regulated to such an extent that we are required to provide in order to ensure that there is a flow of information and business operates as usual.

So having those metrics, and having that information, becomes immensely valuable. I think that one of the complaints that you will sometimes hear from my colleagues in the financial services industry, and particularly in the voice over IP and broadband, is that often times some of the providers do not provide information on outages, or there is a pretty significant delay in providing information on outages.

So having some sort of requirements around what the reporting should be, and what sort of format

it should be in, I think would be helpful in terms of standardizing, particularly among the different telecommunications services that are now part of the fabric of our business, and our communications networks.

MR. GOLDTHORP: Thank you. Laurie or Roger, anything from like a 911 or NG 9-1-1 front?

MS. FLAHERTY: Well, when we talk about emergency communications, it is a system that has three major components. The first is public access, and the second part of that is 911, and the third part are the first responders, and their emergency communications systems.

And unless you have that whole model covered, it doesn't work. They are all absolutely dependent upon each other, and so again going back to what you said, John, without knowing how to characterize how well each one of those is working, it is hard to know how well the system is working as a whole.

And so the reporting piece becomes very important. There are models for that kind of reporting in other businesses as well. I mean, in the auto industry, for example, the agency that I happen to work in, and as a part of, has a reporting

structure as well.

And it is a reporting structure that has requirements, but has voluntary reporting from car dealerships, from auto owners, and all of that data together really creates a picture for how well any particular make or model is doing, in terms of safety.

And I think that analogy has merit in terms of its application to emergency communications. Without knowing how much of a problem it is, or if it is a problem at all, it is really difficult to characterize the reliability of any of those major components.

MR. GOLDTHORP: Thanks, Laurie.

MR. HIXSON: I guess I will just add one comment. Outages are obviously undesirable, and from a 911 perspective, our objective is for everybody to have the opportunity and ability to call 911 and get through when they need to.

The networks and the systems that provide that capability need to be as dependable as possible within reason, but the end result of an outage reporting process to me is that its biggest value, I think, is to find ways to avoid reoccurrence of outages, and try to minimize the number of outages that occur.

And for practical purposes the type of outage reporting that is currently in place is based on how many lines or customers are affected for what period of time.

Theoretically, of course, any customer being affected for any period of time is undesirable from a outage in regard to emergency services. So, using good outage reporting information to analyze what caused it, and how that can be avoided, not only in that particular locality or instance, but in general, is a desirable part of information being used to make the overall service better.

MR. GOLDTHORP: Thanks, Roger. Stacy, do you have anything?

MS. HARTMAN: I jus want to add to that from a service provider's perspective a little bit about our existing Part IV rules today. I would say that across the board that providers today are doing a good job of reporting and complying with the rules as they are written.

CenturyLink as well takes that very seriously, and to the point that was made earlier about being able to share information, or have access to it, that information that we report today under the existing rules is considered confidential, and

certainly the FCC aggregates it, and on a quarterly basis meets with industry, and the Network Reliability Steering Committee, and we review the information.

As well, they bring in issues or concerns that the industry as a whole looks at, and determines kind of where to move forward with. So I think that is another good example if you will of a collaborative effort that has really served us well over the years.

I think that we have gotten very comfortable working together and resolving issues, and I imagine as we move forward into the extension of Part IV that that type of model will continue.

So some of those aspects are key to understand. I know as well with some of the issues around next NG 9-1-1, and 9-1-1 in general, we certainly already have some obligations there that are being reported on, and across the board, and again from at least CenturyLink's perspective, I think we are doing a very good job of reporting and maintaining that.

MR. GOLDTHORP: Thank you. Mr. Fujino, anything to add? I think that you covered a lot of this in your earlier remarks, in terms of your views on what is happening in Japan?

MR. FUJINO: Yes. To have precise

information quickly is very essential for both government and the public, of course, for the countermeasures.

And we are more and more dependent on the IP networks, both for those kinds of public education and for the emergency calls. So it is quite essential in Japan for us, too, to get the information on the IP networks.

MR. GOLDTHORP: So there seems to be at least some level of -- I won't use the word agreement, but I think that might be too strong a word, but at least -- well, I don't know if everybody would agree, but at least acceptance that there is some merit to doing what is done today here in gathering this information, and using it the way that we use it.

It could be made better, I'm sure, as everything can, and we are always open to making it better, and we are trying to make it better now. But let me ask this.

Is there any -- you know, the communications infrastructure is changing under our feet, and John, you made the point earlier -- and what we call broadband is now in use by people across the country for basic services, emergency services.

So it is no longer sort of Next Generation.

It is current generation. And my question then is that now to the extent that we have a technology that is no longer nascent, and it is critical to emergency communications, and financial transaction communications, and in critical sectors like yours, John, why shouldn't -- in your opinion, why shouldn't we be doing the same kinds of things for broadband services and technologies that we do today for previous generation technologies?

MR. CARLSON: I mean, honestly, I can't really think of a good reason why we wouldn't. I think that the point that Laurie made, in terms of understanding the interconnections, and the interdependencies of some of these different networks, and the technologies that go with them, the applications that we are using, in addition to -- at least in the financial services industry, we have to follow our customers in terms of where they are going, and how they are accessing, and how they are using the services that we provide.

And so having a sense for how the pieces interconnect, and where there are interdependencies and vulnerabilities, and outages being one of the important metrics to monitor, I really can't see a strong reason why you would want to have different

standards around broadband than you would from the traditional, the telecommunications services.

And I think that more to a point, I think we need to be constantly thinking about how technology is going to continuously evolve, and we really need to be in the mode of thinking about continuous improvement, and how do we strengthen the networks.

And, in addition, to improving the efficiency and lowering the costs, and all those sorts of things, which has really been a major driver, in terms of the expansion of telecommunications in the broadband space.

But we also need to think about are we looking at the fundamentals, in terms of having reliability of service, and having resiliency in those services.

And particularly in my sector that is critically important, both to be in the business, but also to be heavily regulated, and to meet those different government mandates.

MR. GOLDTHORP: Thanks, John. What do others think?

MS. FLAHERTY: I understand that the industry has a vested interest in providing reliable vested services, and I guess the piece that reporting

adds is a broader picture.

Going back to the analogy that I used before, it is much easier to determine whether or not there is a problem at all, or how large the problem is, if you are gathering information from a number of -- in this case, service providers, and in the analogy that I used, auto manufacturers.

Without gathering information from each and all, it is difficult to figure out whether or not there is a problem at all, or how much of a problem you are actually dealing with.

And going back to what John said, and in terms of managing those things, it is really difficult to figure out how to manage what you can't measure. So from the FCC's perspective, in terms of the statutory requirement to ensure 911 services, I don't know how you would do that without being able to figure out that large a picture.

MR. GOLDTHORP: And thinking about it, maybe you and Roger can think about this in the context of NG 9-1-1, and so while today we have pretty good visibility about 911 services provided over traditional communications networks, as we migrate to NG 9-1-1, that is all mixed in with this, and our visibility there is part of the question.

So what are your thoughts on the importance of applying the kinds of methods that we have used in the past to get the same kind of visibility about 911 services provided over broadband networks?

MR. HIXSON: I think the methods currently in use serve as a starting point for a model, but don't necessarily 100 percent translate into the new network environment for a couple of reasons.

One, economic pressures, and the ability of IP networks to support multiple applications and so on, tends to concentrate critical services into networks where they may have been distributed before.

So where you have IP networks, whether they are public internet approaches, or private managed IP networks, which is NG 9-1-1 public services utilizes, there is a need to look carefully, I think, at the characteristics of those networks, and what they support, and how they support them.

And to use that as a base to consider what different kinds of reporting might be needed in the new IP environment, as compared to today. One characteristic here is that the NG 9-1-1 design that NINA has put forth is based on objectives set 10 years ago, that include the ability for public safety authorities -- and hopefully regional or State level,

as compared to individual counties -- provides the ability for them to set up their own private IP managed network.

And to use that for not only NG 9-1-1, but for IP based radio, poison control, various other emergency services processes and applications, and to do that on a single network.

Now, that network, by its very design in terms of IP, has a lot of diversity and resiliency aspects to it and so on. But I guess my point is that we are tending towards a situation where multiple critical services and support are going to be concentrated on specific IP networks.

And that may affect what should be reported, and how it gets reported, because for those areas, which will be the minority, I think, but still there will be some, those areas where 911 authority is actually buy, build, and operate, and manage, and troubleshoot, their own NG 9-1-1 systems and emergency services networks.

That is a troubling reporting point that has not necessarily been involved in the past, because it has been carrier services oriented. So now you have private systems if you will that are very critical and will have to be dealt with.

MR. GOLDTHORP: Yes, okay. I had not thought about it from that point, and it is almost like today's LMR networks, 911 networks in that fashion, and in a way that you have got privately administered and provisioned -- and for some reason the name is escaping me now, but the name of the network, the local network that is used to interconnect the PSAPs in an area. So, okay, that is a good point.

MR. HIXSON: And we still have certified carriers that are providing into 911 systems that have the reporting connections already there so to speak. You will have vendors who are operating them for public safety authorities.

And in some cases, you will have public safety authorities that are doing it themselves, and so you have three different types of general points where outage reporting would need to be dealt with.

MR. GOLDTHORP: Okay. That is a good perspective. Thanks. Stacy, I will give you an option.

MS. HARTMAN: Sure, and actually, I have a couple of things, just to jump on. Along with what Mr. Hixson was just saying, there certainly is an underlying difference between the Legacy PTSN network

and IP networks.

And that has to be taken into consideration as we move forward with looking at broadband outage reporting and interconnected, and so on, and so forth. From CenturyLink's perspective, we don't believe that it is the right thing to do to apply the existing part for rules exactly over the IP networks.

And we have to look at some of these fundamental differences as we move forward in doing that. As well, the NBPRM, as it is written today, has some issues around a performance matrix being included, and we don't believe that the performance matrix should be utilized as a base for broadband or void outage reporting.

And that really what we need to be focusing on is the loss of complete services, or connectivity, as we are looking at this moving forward.

MR. GOLDTHORP: Well, I was going to ask you if you wanted to comment on either instead of or in additional question, which was why shouldn't it be done.

The other question is if it were to be done differently. In other words, what can be done to reduce the burden, and what can be done to make the proposal more tolerable. So that is a question -- and

you were answering that.

MS. HARTMAN: Yes.

MR. GOLDTHORP: Do you have anything else to add?

MS. HARTMAN: Well, there are a couple of things that I didn't already mention. The first thing as we move forward that I would recommend is that the Commission continue to work with not only CenturyLink, but the industry, to talk about what the appropriate thresholds criteria time frames for reporting are.

I think that we have a pretty good and solid foundation when we went through the development of the disaster information reporting system, and just a good effort to get us to a place where at the end of the day when the system was rolled out, we were already to go, and everybody was onboard with how to actually report.

And it has really been a good, I think, reporting mechanism, and at least the process to get there should be utilized again. As well as from CenturyLink's perspective, it would be beneficial in addition to that, with the industry's collaborative effort to develop a voluntary type of reporting mechanism that essentially could be put in place for a 12 to 24 month reporting period of some sort, so that

we can work out the bugs, and figure out what is working, and what's not, and see whether or not the data justifies essentially moving forward with something that is more mandatory in this realm.

MR. CARLSON: And if I could just jump in. I think that it would be immensely helpful as you go through that, because I think trying to impose an existing standard on kind of a new technology obviously has a lot of challenges, and kinks, and things that you need to work through.

One of the things that I would strongly encourage to both the FCC, as well as the industry, is to keep in mind your customers, in terms of how are they going to use this information, and how can it help achieve the ultimate goal, at least from what I see, as greater resiliency, and understanding what the quality of service you purchase, and what are the capabilities of the services during periods of stress, or crises, or events of that sort.

So that consumers -- and what I am talking about here, I am talking about large corporate customers who can be better buyers, and know what they are getting for the service.

And that we can achieve these public policy goals of having some diversity and resiliency in the

networks, as opposed to just a lot of inexpensive service that during times of crisis may not be there when we need it.

MR. GOLDTHORP: So what are -- well, when we talk about the fact -- and I agree with you that taking the very same approach, and the same methods, and the same metrics and thresholds -- I mean, if you want to get down into that level -- that we use today for communications technologies of the past, and applying that directly tomorrow's technologies and systems, that would not be the right thing to do.

We would propose something different, which takes into account how technologies have changed. And that may or may not be what we end up with, but it is what has been proposed.

So one of the questions that comes -- well, actually, this is something that we are going to get into quite a bit of depth into on the second panel. And, Stacy, you will be on that panel as well.

So I don't want to probe into that too much here, but I do want to ask about the question of a voluntary approach to doing this, because it tends to come up a lot.

And that is what whenever we ask about reporting, and should we extend the reporting rules

that we have, folks will say, well, why not do it on a voluntary basis.

And I guess my answer is always that we did try that once, right, back before we did the original rules in Part IV today. We did that back in 2003 and 2004 as part of -- it was NRIC then, the Network Reliability and Interoperability Council.

And it didn't work out so well. There were a lot of gaps in reporting, and so we concluded that just wasn't viable. Now, Stacy, I don't know if you are suggesting that we just opt for an approach like that wholesale.

It sounds like what you are suggesting is to try it out for a while, but what would you say that the try it out for a while should have a definite end date, and then we roll into something that is more deliberate and more affirmative?

MS. HARTMAN: That's a good question, and first, before I answer that specific question, I will back up and say that today we have in place the Disaster Information Reporting System, which for those that aren't familiar, is a voluntary reporting system that was developed in collaboration with the industry.

And I think that you and I would both agree that it has been a very successful program, and that

carriers are across the board using it, as we should. Granted, I know that it is for disaster situations, which is a little different than the day to day reporting. I understand that.

But I think as well that we have gotten over the last five years to a point where service providers -- and CenturyLink is one of them -- are more in tune with, and willing to go down that road, and report, and do it well every day where we need to.

But part of that gets back to the point of giving us an opportunity to work with you up front so that we can make sure that what you are asking for, we can provide, and if we need to do a little bit more looking, then when we get to an end point where we are all comfortable, and we can provide you what you need, and what we can give to you without reinventing the wheel if you will.

And to your question about the suggestion about voluntary reporting is, and it is something along the lines of let's work together and figure out what metrics threshold programs are going to work to get you what information the Commission needs, and again for the service providers to be able to go back and say this is what we are going today, and this is what we can provide to you via some sort of electronic

reporting mechanism similar to NORS today.

And that we try out -- you know, we know, for instance, with existing Part IV outage reporting, there are some criteria in there that are probably more helpful to you, as far as public safety, and protecting our Nation, versus maybe a single DS3 outage that lasts 22-1/2 hours, and is that as high on your radar.

And we want to make sure that we get between here and there with you so that you are getting what you need, and we are providing what we have. And then the 212 to 24 month period gives us some flexibility to say, okay, this is the criteria time frames and threshold, and we believe are acceptable.

Let's put these in place through this voluntary reporting -- you know, electronic system, and do it, and see does the data actually support the need for moving forward with something that is more mandatory, or does it not require mandatory rules of some sort or fashion.

Is it something that can be handled, and that the industry responds well to in a voluntary fashion, and we could move forward with that. That is my suggestion.

MS. FLAHERTY: A question. Just in terms of

a voluntary system, and again going to or looking at other models, who would you envision being part of that voluntary system?

And again going back to sort of -- you know, the auto manufacturing model. There is a voluntary reporting system there. It also includes consumers, and it includes interim agents if you will, in terms of the dealerships.

So who would you envision being part of that voluntary exercise? Would it be all of the above, or would it just be some of them?

MS. HARTMAN: From my personal perspective, I think it would follow the same subset of folks that are reporting via Part IV today; wireless, satellite, wireline. There is a gamut covered under the Part IV. I would imagine that it would be that same subset.

MS. FLAHERTY: So the service providers.

MR. GOLDTHORP: Okay. We have just a few minutes before I want to start taking questions, and we are supposed to be ending at a quarter-after, and we are going to go a little longer than that because we got off to a little bit of a late start, and that's okay.

Let me ask from John, and Laurie, and Roger, from your point of view what are -- and, you know,

others, but I am thinking what are the kinds of things that -- and you are representing important sectors, you know, public safety and the financial community.

What would be the important things for us to know about as far as outages are concerned in broadband networks and services that you use today and that you rely on today. What should we care about?

MR. CARLSON: Well, certainly to -- and I don't want to repeat myself, but just having kind of core information to make good decisions, both in terms of being a perspective buyer, as well as to be a consumer of service, and understand how these systems operate, and where their vulnerabilities are.

Often times that is something that is learned as a result of having experience with the provider, and really looked at from a risk management perspective, as opposed to having all that information up front before you purchase the service.

So I think ultimately that is what I would like to see it go, is to have the type of information for the private sector to be informed consumers before they purchase.

So that would drive the market towards those that hopefully have a higher reliability. But I also given the complexity of these systems having that

information to help with the risk management process, and the ongoing risk management process, is immensely helpful.

And those metrics get build into how large organizations manage their telecommunications networks, and work with their business units to deliver the level of service that they need, or what is required by regulatory requirements.

So that is kind of the broad -- kind of higher level concern that certainly I have, and would like to see with this. Clearly, there is a lot of details that I am not knowledgeable enough, in terms of the intricacies of the different rules, and how it applies.

And that is where you really need the technicians, and the engineers, and the legal people to figure that out.

MS. FLAHERTY: I don't think I am going to tell you anything that you don't already know, but we really are just at the beginning of NG 9-1-1, in terms of its implementation.

And so it will only get more complex as we move forward. It is a much more complicated system than we started with when that first call was made in 1968.

That being said, I like Stacy's idea of pulling stakeholders together from both sides to talk about the process that would be used, and perhaps not only the process, but the metrics.

And there is sort of a natural push and pull that happens between public safety and service providers that may end up in a really healthy result, in terms of the reporting requirements. So, those two things.

MR. CARLSON: Can I answer back in?

MR. GOLDTHORP: Yes.

MR. CARLSON: This reminds me that some of the models that I have seen have either worked well or did not work well, is if the government could step in, in terms of providing the form to bring the different parties together to try to problem solve in these types of situations with a sustained effort.

There was an exercise that we did back in 2003 which we worked with the National Communications System, which at that time was part of the Defense Department, and was transitioning over to the Homeland Security Department.

And working with the National Coordinating Center, which is all the telecom providers that collaborate together, and it is a real successful

model, and certainly how to respond to disasters.

And we worked in partnership with a lot of the large financial institutions, and actually did a very innovative mapping of the circuits that were telecom service priority circuits, TSP circuits in a particular city, to see where there were potential vulnerabilities in the way that the circuits were mapped, and the way that the telecom providers groomed those circuits.

And we found a number of issues that were then dealt with at the individual level with each telecom provider in each financial institution.

But the point of my story is that that took a tremendous amount of effort, and it was all gratis, both in the telecom side, and the financial side, and it really only would be possible with the support of the National Communications System staff to keep that process going.

So that is one model where you can bring the parties together. The other model which works, but we all hate, is the one where it is voluntary, because you have this threat of some sort of mandate, either a regulation or a law, that really drives the action of the different parties to come together and really solve a problem within certain period of time.

Either one of them work, and certainly people feel more comfortable collaborating, but there has to be support from the parties, because it does involve significant costs, time, and energy for the different parties, and you have got to get that level of support at the top from all the companies on the different sides, as well as from the government.

And in this budget constrained environment. that is really hard on all sides, public, as well as private.

MR. GOLDTHORP: Okay. All right. Thank you. Does anybody else want to add anything?

MS. HARTMAN: I think maybe just one comment back to that. At least from CenturyLink's perspective, I think that we would rather do the work up front to get that taken care of than after the fact of being mandated to do so.

MR. GOLDTHORP: So would we.

MR. HIXSON: I have one minor and potentially meaningful point. At least from a NG 9-1-1 perspective, since it uses IP networking obviously, and it is software, granted, and is not discreet components anymore as E-9-1-1 was, the system itself is going to be able to pattern, recognize, report on, both suspected and real problem conditions if you

will, and it can report a generator to do practically anything that you want it to do, in terms of having available data to roll up.

And that is going to be possible in the future not only in the individually NG 9-1-1 system case, and hopefully a multi-county, regional, or State level type of thing for lots of reasons.

But it is also going to be able to send reports to emergency operations centers at local, State, and Federal, or various other types of Federal entities, such as FEMA, Homeland Security, and so on.

It has the opportunity to do that, and it can do it, and whether it gets done or not is a political curiosity question conceivably. But my point is that it is not necessarily dependent upon the traditional points of information.

The system will be able to sense its own issues, and report on them independently of a baseline transport provider, for instance. So, whether that gets utilized or not for anything other than an aggressive service management, such as outage reporting and other types of issues, and patterning of emergency cases and things of that nature, is dependent upon what we all decide to do.

But the concept there is that there are new

opportunities to measure and report on things that have not existed in the past that may come into play.

MR. GOLDTHORP: Okay. Thank you. And thank you all. What I want to do right now is turn this over to questions both from the floor, and also from -- we don't have anything from the internet? Okay.

So you all will have to be very full of questions today, and I will ask that anybody who has a question to please come up to one of the mikes. There is one here, and one here, and give us your name, and who you are here with, and speak into the mike because this is all being recorded. If you don't have questions, I do.

MR. SALTERS: Thanks, Jeff. Harold Salters, Team Mobile. I have got a question for Peter Carlson for the financial sector coordinating committee. Peter, how do your members use the SLA process to get the kind of resiliency and network specifics that your members are looking for?

MR. CARLSON: Yes. I don't know all the details on that. My knowledge is really dated from a few years ago when we were looking at kind of diversity assurance, and don't have specifics in terms of the broadband applications today.

But back then, they basically couldn't get the assurances that they were looking for, because it was something that the telecom providers couldn't necessarily provide in terms of --

MR. GOLDTHORP: If you could pause for a second.

MR. CARLSON: Yes.

MR. GOLDTHORP: What John is talking about is ensuring the physical layer circuit routing at the physical layer, and not at the link layer, but at the physical layer.

And physical layer diversity and insuring that circuits that are provisioned with diversity don't get groomed in a way that causes them to lose their diversity. That is what you are talking about, right?

MR. CARLSON: Yes, right. And so my point is that there is not a lot of good data that is out there that you can rely upon to make these kinds of decisions.

You get some of it in the sales pitch when you are getting the purchase of it, but often times some of the information coming back is not what people want in the end.

MR. SALTERS: Does the financial sector get

this information from the FCC now, because my understanding is that it is given under confidentiality? In other words, you are looking for the publication of that data?

MR. CARLSON: Well, again, some of the intricacies I am not fully aware of, but the challenge here is making sure that your information is available either on a confidential basis to a company that has a contract with the service, but I am really talking about how do you make consumers, and in this case, large corporate customers, better informed at the purchasing stage when they buy the service, and understanding what the reliability and the diversity capabilities of the service is.

MR. SALTERS: Thank you.

MR. GOLDTHORP: Okay. Anybody else? Okay. Thanks, Harold. Any other questions?

(No response.)

MR. GOLDTHORP: All right. Then I am not going to -- well, I had a couple of more questions, but they are more specific to specific panelists, and so I am not going to go there.

But I do want to thank you all for coming. I don't know what it is like out now, but it has been miserable out for the last few days. So, anybody

having to fly in here, it was a hurdle, and anybody having to drive in here this morning, it was probably not easy either.

So thank you all. We appreciate you coming, and hopefully you will stay for the rest of the workshop, and with that, I will close out this panel. We will then very shortly -- what do we have, a 15 minute break now?

So we will have a 15 minute break now after this panel, and then we will go on with the second panel this morning. Thank you.

(Applause.)

Whereupon, at 11:23 a.m., the workshop was recessed, and resumed at 11:46 a.m.)

MR. MOSLEY: I am Vern Mosley, and I am a senior engineer here at the FCC. What we are going to do with this panel, too, is that we are going to talk about metrics and thresholds.

Basically, the triggers for the outage reporting for interconnected VoIP and broadband ISPs. So, this morning, you heard from the first panel talking about the benefits of reporting, and I am going to talk specifically about how would you trigger that reporting for broadband ISPs, as well as interconnected VoIP.

So we have all the panelists. So the format that I am going to follow for this panel is that I am going to briefly introduce everyone. We are going to allow the panelists an opportunity to make some opening remarks.

Then we are going to have an interactive discussion. We are going to take a pause around 12:30, and we are going to have the Chairman come in and give some remarks.

Then we are going to continue our discussion, and if time permits at the end, we are going to allow some Q&A from the audience, as well as from our viewers through WebAct, as well as from the FCC Live.

Let me give you that e-mail address if you do have questions, and you are watching this remotely. To e-mail your questions, you e-mail them to LiveQuestions@FCC.gov.

So, with that, let me go ahead and introduce our panelists here. First, we have Mark Adams from Cox Communications. Then we have Stacy Hartman, and she is with CenturyLink. Then we have Robert Kondilas, who is from Computer Sciences Corporation.

Then we have Michael Mayernik with Vonage. Then we have Scott Robohn, representing the

Telecommunications Industry Association; and Mike Rowley, from the State of New York Department of Public Service.

So we are going to go now to some opening remarks. First, I am going to start with Mark. Mark is the Executive Director for Technology Operations at Cox Communications, where he leads the corporate technology operations support group responsible for the quality, reliability, regulatory, and operational support systems, as well as application development. So, please welcome Mark.

(Applause.)

MR. ADAMS: Thank you. Good morning. First off, I would like to thank the Commission for inviting us to participate in these proceedings today. As an intro, I would like to give a brief introduction of Cox Communications.

We are the third largest cable multi-service provider in the United States. We have approximately six million customers, where we provide voice, video, data, internet, and wireless services.

We are actually the seventh largest telephone provider in the U.S., with about three million subscribers. On the broadband side, we have about four million high speed internet service

customers, and we interconnect in our markets with a broadband backbone that we own and operate.

We are highly committed to reliability. In the absence of regulation, we have over the last 15 years, we have invested billions of dollars in our infrastructure to make sure that we are delivering the most reliable service to our customers.

We are particularly proud of the multiple service awards that we continually receive from entities like J.D. Powers and P.C. Magazine on the reliability, performance, and customer satisfaction of our services.

While we are committed to reliability, we do have some concerns that some elements of the proposed rulings are excessive, versus cost, versus value, and will not facilitate reliability improvement, which Cox is very keen on doing.

So in the interest of time, I will hold there, and as we get into the questions, we can elaborate on those concerns. Thank you.

MR. MOSLEY: Thank you, Mark. Next we are going to have Stacy Hartman. Stacy is the Director for Federal Public Policy at CenturyLink, where she is the subject matter expert for Federal and State regulatory reporting requirements in connection with

CenturyLink Network Service Outages. So, welcome, Stacy.

MS. HARTMAN: Thank you, Vern. As I mentioned during the last panel, thanks for having me back for a second one. CenturyLink is committed to collaborative work efforts, and really appreciates the opportunity to be here today to talk with the Commission, as well as the rest of the industry, about these service outage issues, and in particular the interconnective VoIP and broadband outage reporting.

We do not believe that Part IV outage reporting should be extended to interconnected VoIP service providers or broadband ISPs. Interconnected VoIP service providers and broadband ISPs have market based incentives that drive them to provide their customers with the most reliable services possible.

Further, they continue to diligently work to develop, update, and implement best practices that are integral to continuously improving the reliability of our services.

Mandatory outage reporting and interconnected VoIP service providers, and broadband ISPs is unnecessary, and the associated costs and burdens for the service providers are not justified by the limited benefits that may accrue.

If we are to move forward with some sort of reporting program for interconnected VoIP and broadband ISPs, as I mentioned during the last panel, it should be a voluntary reporting program that is put in place, and that is developed not only with CenturyLink, but with the industry as a whole.

Any mandatory outage reporting program that is adopted for interconnected VoIP service providers and broadband ISPs should define an outage to be the complete loss of service, or connectivity.

Defining an outage on the basis of performance matrix goes beyond what is necessary if the Commission's objective is ensuring reliable interconnected VoIP subscriber access to 911 service.

Any outage data that is submitted to the Commission should maintain its confidentiality as it exists under the existing Part IV rules today, and as well, we will continue to work and collaborate with the industry in an effort to do so.

MR. MOSLEY: Thank you, Stacy. Next, we have Robert Kondilas. Robert is a Cloud strategist with Computer Sciences Corporation, where he focuses on strategy for private Cloud services, and is an active contributor to the National Security Telecommunications Advisory Committee, Cloud Computing

Workshop, defining the national security and emergency preparedness as it relates to the Cloud. Please welcome Robert.

MR. KONDILAS: Thanks, Vern. I appreciate it. From CSC's perspective, the reason why we are here today and participating in this panel is that since the GETS WPS Program inception, which is now known as Priority Telecommunications Services, we have been concerned with reliability and ensuring resiliency as we see a tectonic shift of moving from the PSTN to broadband.

So our participation in this panel is primarily of interest to make sure that the PTS program continues on, and ensures that the reliability of communications for INSEP continues. Thank you.

MR. MOSLEY: Thank you, Robert. Next, we have Mike Mayernik. Mike is a senior director of network operations at Vonage, where he oversees all incident, problem, and change management activities across the call processing database and web application environment, the network infrastructure, and data center facilities. Welcome, Mike.

MR. MAYERNIK: Thanks, Vern. First of all, I would like to on behalf of Vonage to thank the Commission for allowing us the opportunity to

participate in the rule making process, and secondly, I would like to take a minute and summarize the vonage perspective on the actual rule makings.

So although outage reporting makes sense for traditional wireline services, it is our opinion that it is unnecessary for interconnected VoIP providers such as Vonage.

Due to the extreme competitive nature of our industry that allows customers to change providers in a matter of a few points and clicks, and for poor performance, and the rapid events of voice override peak, voice quality technology, interconnected VoIP providers are highly incentived to design and deliver the best quality reliable networks that they can deploy to gain market share and minimize turn, while at the same time minimizing their exposure to outages that routinely affect traditional wireline services.

However, should the Commission still feel it necessary to proceed down the path of interconnected VoIP provider outage reporting, it is also our opinion that that reporting should be based on a customer's loss of communication services, and an ability to make or receive phone calls, and not based on quality of service measures or thresholds.

The ability, methods, procedures, of

interconnected voice providers to capture, calculate, and report quality of service data today is inconsistent and not standardized across the industry.

And that rapid advances in the voice quality processing technology that smooths over potential call quality imperfections at the customer side would quickly make obsolete any thresholds written into reporting criteria.

So, in closing, Vonage recognizes the Commission's commitment to monitoring the reliability and resiliency of our Nation's communications infrastructure, but feels as those extending outage reporting to interconnected VoIP providers would not further this initiative, but rather consume valuable resources on either side, and force inconsistent or inaccurate reporting from providers, and impose an unnecessary burden on costs on the providers, and possibly customer confusion on the benefits and reliability of interconnected VoIP services.

However, again, should the Commission impose outage reporting requirements on interconnected VoIP providers, then it should be tailored to the customer's lost communications and ability to not make a phone call. Thank you.

MR. MOSLEY: Next, we are going to have

Scott Robohn. Scott is the Director for the America's Technology and Solutions organization at Juniper Networks, where his team provides expertise to Juniper's customers and partners on a wide variety of issues, including IP and MPLS, network architecture, technology, security, and software.

Scott is representing the Telecommunications Industry Association on the panel today. So, welcome, Scott.

MR. ROBOHN: Vern, thanks for the invitation to be here. It is a privilege to be here on behalf of TIA. TIA is an organization with over 500 members that provide network communications equipment and integration services to many of the members of the panel here, and folks in the audience, today.

I am here primarily with my technologist's hat on today. I don't have an official position on some of the specifics that we are talking about, but I can help provide insight into the how, and how some things can be measured, and what levels are required, and how the how should impact the why and the what. So I will leave it at that, and we will have some good discussion.

MR. MOSLEY: Okay. Great. And last, but not least, next we have Michael Rowley. Michael is

the interim chief for network reliability at the New York State Department of Public Service, where his work includes network outage response and analysis, emergency planning and continuity of operations management, field inspection and safety code enforcement, underground facility protection, support of public safety and emergency communications, and participation in Federal and State proceedings dealing with network reliability. So, welcome.

MR. ROWLEY: Good morning, and thank you, Vern, and the FCC for inviting me to this very important and somewhat timely workshop. As many of you know the State of New York and other northeastern States have been over the last 12 days dealing with a major catastrophe.

And we have been facilitating efforts with the Federal Government -- FEMA, the FCC -- and some of the local and regional emergency response units, and our role there is facilitating some of the interactions between the traditional telephone companies, the cable companies, the cellular companies, to get services to the people and the support service agencies that need it at this time.

And I think that a lot of the cooperation that we are seeing, and the good work that is being

done, at least from our perspective, and the ability for us to lend a hand, comes from our outage reporting program.

We several years ago invited the cellular and IP companies to come and participate in our program. We built relationships with them. We do get great reporting in times of need. We would like that to continue obviously.

But I think as far as metrics go that there is a value to measuring the performance of these systems, and again our primary focus is supporting the emergency communities, and that is -- you know, I could agree with a lot that was said, and that they need to be customer centric.

The difficulty we have is that the people that we support are on the lower geographic relevance, and it is sometimes hard for these -- what we call the newer telephone companies, to respond to us, and to build systems to do that, and we recognize that.

We have put in comments in other proceedings here at the FCC to get access to NORS data. We think that can be done in a confidential and protected way so that the States and other entities can get some of the real value of metrics and analysis that is done.

So we obviously support the IP networks and

wireless -- you know, the application of the Part IV rules to those entities.

MR. MOSLEY: Well, okay. Thank you. Thanks, Mike. I think you can see from our panelists that we have here that we have a diverse group. So we have carriers represented, and service providers, and we have integrators, and we also have technologists, and also end-users, and folks that have experience at the State level with outage reporting.

So, again, thank you, panelists. If we can have the first slide up for panel two. What I am going to do is talk briefly about four different topics that we are going to cover within this panel.

We are going to talk about the definition of an outage, and then we are going to drill deep on metrics. What does it mean, and what are the characteristics associated with interconnected VoIP and broadband ISP outages.

And then we are going to talk specifically about the values, or what we call thresholds, associated with those metrics. Then if time allows, we are going to talk about how do you count users in terms of interconnected VoIP and broadband ISPs, that would be affected by a potential outage.

So we are going to try and cover those four

topics during this discussion. The first one here is the definition of an outage. So you can see here on the screen what it involves.

And what I would like to ask the panelists there is whether this current definition of an outage sufficient to define an interconnected VoIP or broadband ISP outage. Is this definition sufficient. This is what we use today.

MR. ADAMS: I would say that over the last seven years obviously we have used this definition on the wireline reporting, and it has worked out well. I don't see any issues with that.

I mean, if we wanted to get more prescriptive, we could refine that to say is it on or off, but in some cases there is a gray area on what constitutes the ability of the service customer, the end-user, to actually use that service.

So I like the definition as it is today and that gives us the latitude, and we always do gravitate towards what is the customer seeing as our real determining factor on how we should measure that. So I think that it works well, and I would recommend that we could stay with that.

MR. MOSLEY: Okay. Any other comments?

MS. HARTMAN: Certainly. I will jump in

real quick and I will kind of tail and support what Mark just shared. I think for those of us who are familiar with outage reporting, we can probably repeat that definition in our sleep at night. We might have nightmares of it for that matter.

And for the most part I would say that it is sufficient for moving forward with a couple of caveats. That it not be expanded in any form or fashion to include performance based metrics to define an outage or triggering an outage report.

As well, we would recommend that any outage in this realm be limited to complete loss of service or connectivity.

MR. KONDILAS: I have just one comment, and the definition, as it is stated, it looks like it is targeting a specific communication provider, where with IP based communications, it is more of a collective offering as it traverses multiple carrier's networks, or multiple provider's networks, and that we really need to encompass that in the definition.

MR. MOSLEY: Okay. Any other thoughts on the definition for a service outage?

MR. ROWLEY: Yes, as I stated earlier, I think that we are -- we lean more towards the customer centric, to the extent that it can be defined, and is

it on, or is it off.

Obviously, degradation of service is an issue for wireless communications, and so while we do focus more on the customer centric, and complete outage, degradation of services is I think a valuable metric.

And what we see a lot of times -- well, it is hard to define a facility, for instance, in a wireless network, and if the facility goes down, what is the impact on customers.

And that is important, at least, you know, at our level to understand that is going on. The other stuff, jitter, and we are going to get into that, and some of the other degradation metrics, are less important to us.

But I am sure that we are confident that the providers are measuring that on their own, and their NOX, and looking to see if there are trends that may indicate a systemic problem.

MR. MOSLEY: Well, it seems like we have had a couple of opinions in terms of including performance measures, or quality of service measures in there, as opposed to just straight out binary, and is the communications facility up or down, in order to determine whether or not there is outage.

If you can put the slide back up that defines the outage. I would like to drill a little bit deeper on service degradation, and try to understand is there a way that we can characterize service degradation.

And let me just give you an opinion that I have and see whether or not you agree with that. I think broadband networks may be a little more resilient to service degradation, meaning that the service could degrade to a point that even though there is not a failure, the information flow between a user and potentially a 911 operator, may be such that it may not be intelligible.

So, help me understand what your thoughts are, in terms of service degradation, and is there a way that we can characterize a broadband service degradation? Any thoughts on that?

MR. ROBOHN: Could I ask for a clarification?

MR. MOSLEY: Sure.

MR. ROBOHN: So pardon my lack of extensive familiarity with what is reported today. Is service degradation reported today as well?

MR. MOSLEY: So it is a triggering event.

MR. ROBOHN: I would think to the previous

question to this, we are going to be in an environment for some time where you will have some wireline users, and some Next Generation technology users, and you want metrics that enable consistency and comparison across the technologies.

In a sense, you care about the service that is delivered, and not how it is delivered.

MR. MAYERNIK: So I think from an over-the-top VoIP provider perspective, there is a lot of different channels that an end-user can take to get on to our network, and then off our network.

So what I mean by that is that I don't think from my perspective in any way that there is a single measure or set of measures that can quantify. Like there is no silver bullet that can quantify what a quality service measure who be for a service degradation.

You have cable modem providers out there, and we have DSL, and we have satellite communications, and they all have different inherent challenges to getting on to our network to process a phone call.

So I don't think that there is anything there, no silver bullet there, that we can just track and report on.

MR. MOSLEY: And maybe you could help the

audience out. The term "over-the-top" service provider, maybe if you could just take a second or two to explain what that means in terms of being an over-the-top service provider?

MR. MAYERNIK: Sure. Essentially today to become a Vonage customer, you need to get your own broadband connectivity, all right? We are not a broadband service provider, per se.

So in your geographic region, you would select the broadband server's provider of your choosing, and then you would sign up for Vonage service, and we would provide you a phone adapter, and you would -- your service would essentially ride on top of one of our partner carriers eventually after it comes in to their network routers.

MR. MOSLEY: Okay. So thanks for the clarification.

MR. ADAMS: By the way, on other points, we would agree that performance indicators like PAC, Loss, Lightsey, and Jitter, are not good indicators for indicating is the service available to the end-user or not.

For various reasons, we quote differences in technology. You talked about redundancy and resiliency, and we can generally route around those

types of things. So for those reasons, we don't believe that is a good criteria.

We would stick with the is it on or off, and is the user available, and has the capability to use that service.

MR. MOSLEY: Okay. So the difficulty I think lies in the degradation itself, and what the user is experiencing. So in the case of the example that I used, where a caller is calling into a 911 operator, and maybe there is some service degradation, such that the 911 operator may not be able to understand what the caller is saying.

Since that is a service degradation the line is still available, or essentially the session is available in an IP environment, would you consider that to be an outage?

MR. ADAMS: If you go back to the current definition of significant degradation, we always gravitate towards what is the customer experiencing, right?

So typically, you know, we will get calls and there is this gray area, and is it usable or not usable. Well, I always gravitate towards if the customer says it is not usable, it is not usable, and we will treat it as an outage.

I mean, they both get treated with high priority, but we always go towards the customer's definition.

MR. MOSLEY: Okay. Any other thoughts?

MR. ROWLEY: Well, just to compare the way that we would see it in a traditional telephone network, yes, if the 911 center is not getting or doesn't understand calls, we would certainly consider that an outage.

Now, individual calls, we don't want to get down into that granularity, but if the degradation is affecting calls in a geographic relevant area, and certainly if they are affecting 911 calls, we would like to hear about that.

Again, I think the companies have very sophisticated NOXs, and if that is occurring, we are assuming that they are getting hit with customer complaints, or customer notifications about the degradation.

And in a traditional network, there are certain algorithms of thresholds; you know, 25 calls per area, or a hundred calls per area. And with that, I think the companies can design and engineer that into their systems, and be able to report on that in a geographic area that is relevant to the emergency

response community.

MR. MOSLEY: Okay.

MS. HARTMAN: Can I add something?

MR. MOSLEY: Sure.

MS. HARTMAN: Okay. So something that I just want to point out. That service degradation and generally useful availability, in general, are really not objective standards, which is where we struggle.

At the end of the day, service degradation, and generally useful availability, vary by individual, and who is actually trying to access what. If I am as a user trying to access e-mail, or load a webpage, that service level if you will is a little bit different than, say, I am trying to do a video, or chat, or an on-line game, or something to that extent.

So again it really comes down to the user, and what my specific definitions are, and that is another reason why from our CenturyLink standpoint, we don't believe that we should go down the path of utilizing metrics as a threshold in that form or fashion.

MR. MOSLEY: Okay.

MR. MAYERNIK: So to add on to that, your example does fit the criteria of a service degradation, but to Stacy's point, and to Mark's

point, it is a subjective measure that we are looking at. There is nothing definitive that is going to say it is an outage.

MR. MOSLEY: So what are the objective standards then? Can you name a few, or give me a few examples of maybe what you are talking about, since you are saying that these may be subjective -- quality of service, performance, metrics -- but what are some objective measures?

MR. MAYERNIK: I would just say a customer's inability to make or receive a phone call, or an emergency 911 type call, and essentially figuring out a way to best measure and categorize that, and an ability to make or receive calls. Lots of physical infrastructure, and power, and things of that nature.

MR. MOSLEY: Okay. Any other thoughts? I'm sorry, Mike, but could you repeat that?

MR. MAYERNIK: Sure. I think what an objective measure would be is the inability of the customer to make or receive a phone call due to some type of infrastructure, facilities type issue, power, equipment failure, things of that nature. It is from my perspective a black and white thing, and that I can't make a phone call.

MR. MOSLEY: Right, you either can or can't?

MR. MAYERNIK: You can or you can't. Everything else from my perspective is subjective. So the quality of service from what I am hearing might be different from what you are hearing.

MR. MOSLEY: Mike.

MR. ROWLEY: I think what we heard from a lot of the panelists this morning is true here. There is really two types of reporting that we see. It is the immediate on or off reporting, and again that is the most important, we think.

And then there is other post-event or trend analysis metrics that are important, too. In the telecom networks, we look at customer trouble report rates. We look at some of the service quality type, or service quality centric metrics.

And I think that when looked over time, they give you some insight into what is the reliability of that network, and we do measure and do get at least for video services companies that will file on a quarterly basis that type of information.

And I think that it does, when you look at it over time, or specific to a geographic region, it does give you some indication of reliability.

MR. MOSLEY: Okay. We are kind of talking now about the subject of metrics, and so what I would

like to do is kind of segue into that, and maybe ask some of the service providers what type of metrics do you monitor, one, and present maybe to your network operations center.

And then, two, what types of metrics do you reflect back to your customers? So, what do you monitor and report to your NOXs; and then, two, what do you reflect back to customers?

MR. MAYERNIK: Well, first off, we don't report anything back to our end-users, our customers. They are not getting any quality of service, or metrics type reporting back.

We do capture quality statistics, a certain number of quality statistics on every phone call that goes through the Vonage network via our media relays. Primarily, we are looking at Jitter and Packet Loss.

So those are the measures that we are capturing on a real-time basis for every single call, and if thresholds are violated, it does get reported to our NOX.

And let me just add on a little bit to that. We are blind to what I will refer to as the on-ramp and the off-ramp pieces of our network. So getting on to our network via either a gateway or a border router, and getting off on a boarder router or a

gateway, when it gets off of our network, and it gets off-net, we are blind to those quality of service statistics, and we are not seeing or generating alerts on those.

MR. ADAMS: So, at a basic level, we obviously do device level monitoring, and based on the types of devices, we know generally -- not always, but generally -- is it completely service affecting, or is it going to result in some kind of degradation. So we do device level monitoring.

We monitor our end points for on or off status right through the switches, and through our cable modems. For the customer side, if you look at those customers that are our high-end business customers, we generally do have service level agreements in place, and contractual agreements in place, where we would report certain things.

Generally, it is around attributes, like the number of outages in a quarter, and how long it takes us to respond and restore those outages, and then trouble calls.

So those are the general types of metrics that we might or would report back to the customers that have those agreements in place.

MR. MOSLEY: Okay.

MS. HARTMAN: And then I will say from CenturyLink's perspective, our monitoring and management program is very similar to what Cox just spoke about.

But it is also important to point out that our companies have very robust network management and event response centers. This is their day, 24-by-7, 35 days a year, to make sure that our network is working in the fashion that it is supposed to be working.

And where we have issues, we respond as quickly as we can to get them resolved, and where we need to work with our customers to keep them informed, we certainly are doing that already.

MR. MOSLEY: And if I could ask Mr. Rowley if -- well, from your perspective, what types of metrics are reported to you at the State level?

MR. ROWLEY: As I said in the previous response, customer trouble report rates are important. We do look at outages, at outage events, and the frequency of those events.

Again, some of the minute degradation metrics quite frankly are of no use to us, unless it is impacting service. but again I would think that the companies are looking at that in their NOX, and

that is what I am hearing.

And we don't want everything. We want the important stuff, and we want to be able to react to the important stuff. But we do have certain needs, and I think the Commissioner earlier mentioned the Smart Grid, and the other panelists mentioned the Next Generation 911.

Those are areas that are vitally important to the States, and during this transition between -- you know, a lot of these services are going to be on traditional platforms and IP platforms.

It is going to be very important for us to understand how these networks work, and what is troubling them, and what steps can be taken to mitigate them. And again you can't manage it if you are not measuring it.

MR. MOSLEY: Okay. One of the response that you said, Stacy, was that your networks are robust, and if you look at a continuum of an outage from maybe a possible service degradation, and all the way up to a complete outage, would you agree that service degradation may be an early indicator of a potential outage?

And so maybe that is the type of information that your NOX are acting upon when they are looking at

the various metrics associated with some type of service degradation.

MS. HARTMAN: In some cases, I agree that is probably an accurate statement. Where I think from a service provider perspective, when we get into the IP world, I think that you touched on this just to begin with.

I mean, the networks are vastly different, and the ability reroute around a trouble is much more dynamic in an IP sense, and by the time -- and I think Scott was touching on this a few minutes ago, but by the time that it actually reroutes around and gets to the customer, it is not necessarily the path that it took to get to the customer.

The customer may not have even recognized that there is an issue of any sort that is going on, whether it is Latency, Jitter, or delay of any sort. So from that perspective, you can't say that just because you have some sort of degradation on the up front side of it that it is necessarily going to result in some sort of customer impacting issue.

MR. MOSLEY: Any other comments?

MR. ADAMS: Yes, I agree with that. I think that most service providers would certainly -- well, what we do is we do look at proactive trends, like

call rates.

And the idea state is for us in our monitoring centers to pick it up and address it before it becomes customer impacting. That is always our goal. So we do look at tools, and statistical methods, and things that we can do that would prevent us from having an outage in cases that we can actually take action.

So it is always a desired goal to prevent the outages from ever happening in the first place.

MR. MOSLEY: Okay.

MR. MAYERNIK: And I would like to say essentially the same thing. That is the job of the NOX, and the job of network management, and the control centers, is just to keep the finger on the pulse of the network, and proactively reroute traffic when they start to see a problem.

MR. MOSLEY: I am going to go ahead and put up a couple of slides that we have here regarding the metrics, and the proposed thresholds so that we can further discuss the specifics of that. I will go ahead and take control here. So if you can go to the next slide.

(Pause.)

MR. MOSLEY: What we are going to do is look

specifically at the metrics and thresholds that we have defined for -- and this is for interconnected VoIP. So I will give you a second to look at that.

(Pause.)

MR. MOSLEY: And if you go to the next slide here for broadband internet access providers, it talks about the metrics and thresholds. And then for backbone ISP service.

So for interconnected VoIP, and for ISP access providers, broadband access providers, as well as backbone, here are the metrics, as well as the proposed thresholds for those.

So I think that this is probably a good point to take a break. We are going to pause.

MR. BARNETT: Speaking of outages, this is a temporary outage so to speak, and for a very good cause. From the time that Chairman Julius Genachowski entered office over two years ago, he has placed a priority on public safety communications from two aspects.

One, supporting public safety of officials, first responders, and their communications, but also supporting communications that support the safety of the public, whether it is 911, or any other type of communication.

Mr. Chairman, we are so glad to have you with us today, and please, I offer you the podium for your comments. Thank you for being with us. Chairman Genachowski.

(Applause.)

CHAIRMAN GENACHOWSKI: Well, thank you. Well, first, thank you, Admiral Barnett, for organizing this workshop, and just for the constant work that you and the Bureau do around the clock on these issues.

And I think this combination of public workshops, and engaging with first responders, and carriers, in all sorts of ways, and doing the kind of work that I have seen you and your team do firsthand in times of crisis, like two weekends ago in our ops center.

And the commitment and dedication that you and your team bring to these incredibly important issues is outstanding, and I really honor your service.

Thank you all for participating in today's workshop. Of course, it couldn't be more timely. In the past two weeks, we have experienced major events that have put our Nation's communications infrastructure to the test; a hurricane and an

earthquake in the northeast with a five day span, followed by Tropical Storm Lee, which hit the Gulf Coast this week.

These have had serious consequences. More than 50 people were killed by Hurricane Irene, and countless thousands have seen their homes and possessions destroyed by flooding.

I want to offer my condolences to the many people who have suffered as a result of these storms. Again, Admiral Barnett and your team at the public safety bureau, working around the clock with FEMA, and our other Federal and State partners as part of an intergovernmental effort to prepare for and respond to these events.

Many of you in attendance have been working overtime, too. Thank you for your efforts on behalf of the American people. These recent events have confirmed once again the importance of communications networks in times of crisis, both for first responders, and the general public.

They also confirm that newer forms of communications, like mobile phones, and broadband internet, are increasingly important when disaster strikes.

In two weeks, the Commission will address

proposals to accelerate Next Generation 911. Next Generation 911 will upgrade 911 to seize the opportunities of these new technologies.

We have been working on this and other areas. This was scheduled before the recent events, but of course, Commission consideration of this notice in two weeks will be very timely.

The earthquake and Hurricane Irene brought a number of emergency communications issues to the floor. In general, these are issues that we have been focused on at the FCC.

Two examples are the subject of today's forum, network reliability and outage reporting. These are the focus of ongoing FCC proceedings that the Commission launched earlier this year, and what you are doing today is a very important part of that process, and I thank you again for participating.

As the FCC has done an initial review of Hurricane Irene and the earthquake, it is clear that a lot worked effectively and played a vital role in emergency response.

For example, the FCC successfully deployed several roll call teams, which used especially equipped SUVs to survey damage to mobile networks, enhance situational awareness for first responders,

and identify mobile infrastructure in need of repair or assistance.

The investments that we have made in roll call provided important benefits in the recent storms. The hurricane and earthquake also shed light on ways that we can continue to enhance our work to ensure the reliability of communications during and following disasters.

Three areas for followup. First, the earthquake confirmed the importance of focusing on 011 calls made over mobile networks. Americans increasingly rely on mobile communications, but some wireless networks experienced congestion following the earthquake, and congestion that prevented some 911 calls from going through.

For this reason the Next Generation 911 notice of proposed rule making that we take up this month at the Commission, will also address 911 prioritization.

And I will task CSRIC, the Communications, Security, Reliability, and Interoperability Council, with providing recommendations on how to ensure that 911 is available when disasters spark a surge in mobile network use.

Second, our two outage reporting systems,

DIRS, and NORS, provided good information quickly in the recent events. This information is used to provide situational awareness regarding network outages to the FCC, and also to FEMA, and others responding to a disaster.

The ways that consumers communicate are changing. A growing number of people, of course, are cutting the cord and replacing their phone lines with mobile service, and others are using VoIP and cable for phone calls.

We want our outage reporting systems to keep pace with those changes. Our experience with the recent events will inform our pending rule making on outage reporting, which considers improvements to NORS, including expanding the system to VoIP and broadband outages.

The experiences and lessons in the last few weeks will also inform a separate, but related, inquiry on network reliability. In the wake of the recent hurricane and earthquake, we have been meeting with carriers and service providers on these issues, including outage reporting, and I expect that this will lead to improvements in DIRS and increased participation in the program.

Third, the recent events underscored the

importance of public education about how best to prepare for and respond to disasters. For example, people can help themselves and their families in the event of a power outage by making sure that they have charged batteries available for their mobile device.

We can do more to help people focus on tips like that in advance and other useful information. I have spoken to FEMA Administrator Craig Fugate about this and other issues, and the FCC will be working with FEMA and other Federal partners to develop a single set of tips for emergency preparation and response related to communications, and to use broad distribution channels and public education programs to reach as many people as we can with a single common set of tips.

The steps that I have outlined here can help save lives, and I look forward to working with all stakeholders to get these things done. Thank you for the chance to address this workshop.

I again appreciate the work that you are all doing. It is a very, very important part of our ongoing efforts. Admiral Barnett, thank you again, and I return the podium to you.

(Applause.)

MR. BARNETT: Thank you, Mr. Chairman, for

those timely and important remarks, and we will now resume our regularly scheduled program, and turn it back over to Vern. Thank you so much.

MR. MOSLEY: Thank you very much. So if you will recall, we were talking specifically about metrics, and what I would like to do is talk specifically about the proposed metrics that we have chosen, specifically Packet Loss, Latency, and Jitter, to describe service degradation.

And I would like to get your thoughts specifically on those chosen metrics, Packet Loss, Latency, and Jitter. Well, first, let me ask you this. What do you think about those chosen metrics themselves as metrics to describe service degradation?

MR. MAYERNIK: The metrics themselves may be meaningful, but again I don't think from a Vonage perspective from an over-the-top VoIP provider that there is really any way for us to measure end-to-end on a particular call.

Again, I am blind to the on-ramp, and I am blind to the off-ramp. I only have what is in the middle, and there is no method for me to collect the end-to-end statistics, and so I can't get you a meaningful measure for that, all right?

And I would also like to see the definitions

again just to kind of refresh my memory, in terms of the --

MR. MOSLEY: If we could pull those slides back up for interconnected VoIP.

(Pause.)

MR. BARNETT: All right. There you go. And maybe, Mike, while you are looking at that, maybe I could ask either Mark or Stacy to comment. So if Vonage can't see essentially the underlying network, are you able then to see these performance degradations, in terms of Latency, Packet Loss, and Jitter, in the network?

And are they meaningful from a service degradation standpoint to measure those?

MS. HARTMAN: I will start, but Mike makes a good point. At the end of the day, we only all have visibility to what is on our own networks, and we can only then monitor, and manage, and respond to any issues that we are seeing on our networks.

And there are certain ports where, for instance, as an ISP broadband provider, I am going to pass my traffic off to a different carrier, and I am not going to see the whole end-to-end, and I think that is exactly where Mike was going.

So from that perspective as well, when you

get into the performance metrics that you are talking about -- and I think that you have heard me say this several times this morning, but from CenturyLink's perspective, we don't believe that those performance metrics should be part of any type of outage reporting mechanism criteria or threshold.

MR. ADAMS: I would also echo every comment that both parties have made. It is not a good indicator of a significant enough degradation that would prevent the end-user from having the service available for various reasons.

There is technology differences, and we talked about that, and differences in technology, and we have resiliency and redundancy in place. Again, the viewpoint of being able to see end-to-end, which was the other two comments. So we don't believe that it is a good measure at all for that reason.

MR. MOSLEY: Okay. Any other comments regarding those specific chosen metrics?

MR. ROBOHN: Sure. A couple of things to point out in light of his visibility issue. One thing that we haven't touched on is what end-users do in their homes.

Some more technically proficient, and some less technically proficient, may cause problems with

their ability to access voice services that may just exist in their premise that is beyond the scope of any one of the providers to deal with.

So that is a sticky wicket to deal with in this whole situation. Regarding the measurements and the capability to measure them, taking it at its extreme, there is a lot of data to measure.

VoIP is one application among many applications, and how do you weed through general Packet Loss, Latency, and Jitter measurements, versus just VoIP.

And there is more than one flavor of VoIP, too. you know, different providers might do this differently. So there are many layers to the onion to peel down here that just show more complexity. That is my take.

MR. KONDILAS: Vern, I think it shows that we -- and I understand Stacy's and Marks's point of view, is that across their network that they are looking at -- that they can only measure across their network.

But then as I mentioned before, when you have multiple networks, multiple providers, that are along the route of the call, it is very hard to measure end-to-end performance, which is why the

definition probably needs to go back to the collective performance across the networks.

And so there has to be a synchronicity as to when a call originates on Stacy's or CenturyLink's network, and then terminates on Mark's network, or Cox Enterprises'.

How do we measure each of those legs? It is almost like in IP networks when you measure hops, and what is the latency on the hop, and then is the packet lost, and you don't get to its end point.

And we just have to have that coordination of being able to have traceability going from end-to-end in order to then get a collective understanding of the performance of the call, and if there was degradation.

Because it could be great going across one provider's network, and then goes through the peering point to the other network, and then falls over, and then who is to blame.

MS. HARTMAN: And then I will add in on that. The biggest concern from our perspective with the scenario that you talked about is that we lose complete visibility once it is off of our networks.

So to that end, it could have gone completely across our network without the issues as we

handed it off. We have no insight into that.

MR. MAYERNIK: I would also like to make a comment here, but even though Packet Loss, Latency, and Jitter, are inherent problems with networking today -- they are always going to be there -- companies like Vonage are putting a lot of time and effort into engineering ways to smooth out those imperfections on the network, and that are imperceivable to the human ear.

We do things on our border routers, and on our gateways with jitter buffers that smooth out those inherent problems. We also work with our chip vendors on the devices that we set up at home, and put a proprietary cord on there to help smooth out problems that are inherent on a network as well, either the whole network, or the local provider's network.

So as we talk about these measures and are they meaningful, they might be meaningful, but providers like Vonage are constantly evolving the technology to smooth that out so that they are not perceivable.

MR. MOSLEY: Well, let me talk specifically now about the thresholds themselves, and values, and I will start the conversation by talking about the thresholds that we are proposing for the metrics that

we have proposed.

And then maybe what I will do is I will ask you to comment on if there are any other metrics, or specific thresholds, for any other indicators that we should be considering either in addition to, or as a substitution for, the metrics and thresholds that we currently propose.

So the thresholds that we are proposing for Packet Loss is one percent, and for Latency, it is a hundred milliseconds, and that is measured roundtrip, so that you take into account the acknowledgement that comes back from the destination.

And then for Jitter, it is four milliseconds. So, one percent packet loss, and a hundred milliseconds for roundtrip for Latency, and four milliseconds of Jitter.

And the question is are those essentially benchmarks across all technologies, or should we take into account differences in the different technologies? Like, for example, wireless, or satellite, or any of those things? Does anyone care to comment specifically on those chosen thresholds?

MS. HARTMAN: I can start.

MR. MOSLEY: Okay.

MS. HARTMAN: From CenturyLink's

perspective, we don't believe that those particular metrics are consistent with degraded wave quality, and our a little bit troubling to us in all honesty.

There are a lot of facts that we have already brought attention to today that really affect the performance of VoIP, and are really outside of the control of a service provider.

Some of those are the subscriber service provider, and other entities, and some are facilitators, and for anybody who has read CenturyLink's comments to the NPRM, we did suggest some alternate criterion threshold to consider.

We do believe that the 900 thousand user minute as a threshold for VoIP is appropriate and should be considered, and that there shouldn't again be service degradation embodied in the definition of an outage for interconnected VoIP, and that there should be at least 7,500 interconnected VoIP subscribers that have lost connectivity for at least 120 minutes.

MR. MOSLEY: Yes, Mark?

MR. ADAMS: Given again all the differences in technology, it seems like this is -- and again we are opposed to this. It is not a good indicator of telling are we really not providing the service or

not.

But if you look at the multitude of tools that a network monitoring center has at its disposal, again, we look at many different things. We do statistical trending, and we look at call volumes.

I mean, service providers are very good. We have highly reliable networks. So instead of being specific and specifying a specific level, I would go back to the general definition of do we have a significant degradation that impairs the ability to enable and maintain a communications channel.

Service providers figure that out, and if we didn't figure that out, we wouldn't be in business, right? So we have a multitude of tools. It feels like we are getting too specific here, and it is going to box us into a corner.

MR. MOSLEY: So do you feel that we can have a very objective measure applied to that definition then for significant degradation?

MR. ADAMS: Well, again, some of the comments were that maybe we want to revise that definition to be more specific, and not subjective to say is it on or is it off. That is another avenue that we could take.

MR. MOSLEY: Okay.

MR. ADAMS: We are actually okay with either definition.

MR. MOSLEY: What I would like to touch on next just quickly before we open it up to briefly some Q&As. Counting users in a broadband environment. We mentioned that 900 thousand user minutes was still a metric and a threshold associated with triggering an outage event.

So if you look at different ways that users could be counted, how does that concept apply in an IP environment, especially where you can reuse IP addresses? Does anyone care to comment on how you can count users in a broadband environment?

MR. ADAMS: From a cable perspective, we have a unit, either EMTA in the house, or MTA, and that is the portal that everything connects to. So if we were to look at how many VoIP lines were impacted, we would look at how many EMTAs, which are the subscriber based equipment, and we could look at that. Now, what is behind that, we have no visibility of.

MR. MOSLEY: Okay. Any other thoughts?

MR. MAYERNIK: From our perspective, we ask that our customers keep their database of record up to date with us. So we can tell geographically MPA and NXX, and how many users are in a specific affected

area easily enough.

But if they pick up that device and they go to Mexico or something like that, then we really can't track the movement of it. But we are really depending on them to keep their records up to date from where their home devices are.

MR. MOSLEY: Okay. Thank you.

MR. ROWLEY: Obviously the customer impact is the most important metric for us, and to the extent that it has some geographic relevance, or even at a glandular level, if it is affecting what we would call a major customer, like a 911 center, or a major business customer, or even a utility, those are really key indicators to us.

And to the extent that that can be implemented in the requirements, we certainly support that. We know that in wireline that it is a lot easier to determine the street, and number of outages, and impacts, and we would still like to see that in the IP metrics.

MR. MOSLEY: Okay. Well, thank you. I think what I will do now is go ahead and open up the floor to a few questions. If anyone in the audience has a question, if you could step up to the mike, and announce your name, and company affiliation.

We do have a couple of questions from some of the folks that are monitoring via WebAct, and so we can do that. Yes, sir?

MR. SCHRYACH: Good afternoon. My name is Paul Schryach from Buckeye Kimball System, Toledo, Ohio. As a small operator, I have a number of unique questions and comments.

But as the panel talked about all of the measurements and impairments, it all focused on voice, and I am struck with the fact that voice is simply one more application on a data network, and thresholds that impair an application vary with the application.

Streaming media is going to be very different than a web session, for example. And I am curious how the panel would look at measuring impairments given the different uses of the network by different customers.

And, secondly, as we look at trying to measure this across the network, and track this, as a small operator our resources are very limited as to the development of these tools.

And in a world where our traffic is growing from a customer perspective at about 120 percent a year, we are spending huge amounts of capital just trying to keep up with the customers that we have.

So I am interested in what the panel might suggest for a small operator on how we can begin to pull some of these pieces together and collect the data that the Commission is looking for.

MR. MOSLEY: Thank you, sir. So the first question to the panel is then, if I understood your question here, is that if we look at an application other than voice as an application that rides over the IP, we have kind of concentrated on some of the metrics and thresholds around that, how would you measure impairments for applications other than voice.

MR. ROWLEY: If I can just jump in quickly. Voice obviously is our primary or most important service that we look at, but as other services, such as Next Generation 911, is going to deal with multimedia transmissions, the Smart Grid is going to be delivered over IP networks, and then data becomes more vital to us, and whether that data is getting through or not.

It is going to be a challenge, I think, but it is something that we are going to -- you know, it is just so vital that we are going to need to have some measurement, and oversight, and measurement over that.

MR. ADAMS: Yes, generically, and I think

going back to the response that I gave on the network monitoring, we have multiple tools, and methods, and processes, and statistical methods, and analyzed call volumes, and all kinds of different things that we do.

And that is irregardless of what service it is, and so I think that those equally apply to every service that you have. Now, some of the tools will obviously be different, but you have to use a multitude of things. There is no one silver bullet.

MR. KONDILAS: You know, I think that when you get to the root of where we are talking about Packet Loss, and Jitter, and Latency, and the different applications that the gentleman asked the question on, and if there is video, and there is instant messaging, and things like that, there are some that are less tolerant to Packet Loss, such as video.

If you have Packet Loss on video, you get artifacting, and iconization, and things like that. So I think that there are different levels of tolerances based on the application, and its resiliency to recover.

I mean, if you send an instant message, it goes through because there is not a time sensitivity to it. People don't wait five minutes for an instant

message. They might wait a couple of more seconds.

But with video, waiting for that packet to show up one second later causes or impacts the quality of the service. And I think when you look at the three different measures, that those are the root of how do you make a comparison between what we are used to today -- you know, voice communications -- and a change in the underlying infrastructure, which is moving from a circuit based, circuit switch, to a packet based network.

MR. ROBOHN: And to Robert's point, even within an application, everything is not applies to apples. For example, if we -- and not to disregard the request to look at other applications just within VoIP, but there are different vote coders that react differently, and different Packet Loss conditions, and different Latency conditions.

And one operator may choose to use one set of Codecs and protocols, and one operator may choose to use another, but again, setting a single threshold for any one of these metrics, even in just one application area, might smooth over too many bumps when those bumps really make a difference. The same thing goes to video to even a greater degree.

MR. MOSLEY: Okay. Thanks. And then maybe

for the second part of the question there. Any advice or any major differences in terms of outage reporting that a smaller company would face, as opposed to a larger company?

MR. ADAMS: I think that the gentleman said it well. It is just relative to the amount of capital that companies have to invest in monitoring systems.

MR. MOSLEY: Any other comments?

MR. ROWLEY: From the telecom perspective, I think that some of our cable rules, they do differentiate small systems from larger systems. Obviously, you don't want to set up a complicated metrics reporting requirement that is going to be a burden.

And part of the problems that we have had in trying to get some of our cable providers into our voluntary system was -- and some of the other companies in wireless, was that they would just give us the FCC reportables as they are called.

And we could spend all day getting those, and it is not that useful, and again, it is probably useful to look at over time. I think that the smaller companies -- you know, we do have quarterly reporting rather than monthly and daily reporting.

I think that you want to keep it to where it

is not a burden on these companies to the extent possible.

MS. HARTMAN: Just one more thing in response to that. There are a lot of industry forums where discussions like that occur. I mean, TIA is up here, and they are certainly a good forum. CTA is in the audience, and ADIS is also another one that focuses on these types of issues, and would be a good forum for discussing further.

MR. MOSLEY: Well, let me go ahead and close out the panel then. I would like to thank our panelists for their insight and contributions. I want to remind you that we are going to break for lunch now.

We need you to be back at 1:45. We have Commissioner Copps, I believe, who is going to give some remarks. So, please return back at 1:45. So, thank you.

(Applause.)

(Whereupon, at 12:54 p.m., a luncheon recess was taken.)

//

//

//

//

A F T E R N O O N S E S S I O N

(1:49 p.m.)

MR. GOLDTHORP: I hope everybody had a relaxing lunch, and thank you all for coming back. We have the pleasure this afternoon of having our fourth Commissioner come and speak with us today about these topics.

Commissioner Copps has been interested in these kinds of matters since I have been here. I have been here for 10 years, and I have heard about you talking about this stuff for 10 years now, and I think we see pretty much eye-to-eye on all of it.

So I am really glad that you could make it down to join us and share your thoughts with us, and I will turn the floor over to you.

COMMISSIONER COPPS: I appreciate it. I guess most people have had time to come back, and we need to take an outage report here to see who is here and who isn't. I don't know.

I just want to take a minute to sort of come down and say how pleased I am that this workshop is taking place today. It is a pleasure to be here, both as a Commissioner, and as a citizen, to see government, and service providers, and advisory groups, and academics, and a whole bunch of people

coming together, to tackle the single, most important issue on an FCC agenda that is already crowded with important issues.

And that would be of course public safety, and this could not be a more timely workshop coming on the heels of the events of the past couple of weeks that have reminded us very pointedly about the importance of reliable communications during times of crisis, whether it is East Coast earthquakes, or hurricanes, or tropical storms, or fires.

And this weekend, of course, we all paused to commensurate the tragedy of 9/11. So we have to use this confluence of events to find solutions that will protect our country in times of emergency.

But it is also true, I guess, that we shouldn't need events such as this to remind us of what our duty is. I worked for many years up on Capitol Hill for Senator Fritz Hollings, and he was found of telling us very frequently that the safety of the people is always the first obligation of the public servant.

And he really believed that and he instilled that belief in me. Public safety is both a private and a private responsibility. It is the responsibility of each of us, and all of us as

citizens, and I am pleased that so many folks in the private sector do take this challenge seriously.

Service providers, of course, have incentives to make their investments reliable, but I also believe that they have taken their responsibilities to their consumers by and large seriously.

But the experiences of the past few weeks I think demonstrate very clearly that many citizens encountered serious communications problems. During the recent earthquake, communications in this area were seriously disrupted.

Speaking personally, my daughter, who just was beginning her teaching job out in Silver Spring, Maryland, when the earthquake hit, tried many times to call her mother and dad, but she was connected to wrong parties at numbers that she didn't even call.

Many people experienced a lack of dial tone, and many people experienced a lack of connectivity. The truth is that we don't really know how networks perform until they are tested, but your job and my job is to plan as best we can, and to learn from our mistakes. Our country deserves no less.

So that's why I was pleased to support last May the NPRM, exploring network outage reporting for

VoIP and broadband services. It is long past time to my way of thinking for us generally to get beyond thinking about critical communications as just traditional voice, and it is time to realize that consumers don't make a lot of these distinctions that so often fixate us here in Washington, and that stymied us here in Washington.

And especially that they don't make them during times of crisis, and when they are in trouble, and when they need action fast, and they expect to communicate using all the tools at their disposal, and certainly they expect to get and should get the critical information they need through their IP based services.

So we share a duty to think creatively about how we can arm consumers with additional ways to communicate during disasters. Now, while it may be a little bit beyond the scope of today's meeting -- I don't know -- I will raise just one example.

I think that it is time now for a thorough, calm, and reasoned discussion about FM chips in handsets. We all acknowledge the need for redundancy in communications, especially emergency communications, and last week during the earthquake, a lot of folks were only able to get information through

radio broadcasts when the phone networks got congested.

So what are the pros and cons of an FM chip, and to what extent have other countries had experience with them, and if they have, what has been that experience, and what can we learn from it.

As I say, I think it would be nice if we could have this in a calm and dispassionate, and perhaps a Commission led way, and I just get into one lobby versus another lobby saying all the usual things that you can expect from each of them, but really to look at this as a substantive matter as an opportunity perhaps, if it is an opportunity.

But let's find that out. Why are we waiting. We ought to be looking at any and all ideas that sound reasonable for the protection of the American people, and we have to understand the sense of urgency that is required.

We are a decade now beyond 9/11, a full decade, and I think we have made some progress, and there is no question about that, but we have not made enough progress.

We need to make more and we need to get the public safety -- the interoperable public safety network built. I would certainly hope by now, by the

10th anniversary of this, that we would be a little bit further or a lot further down the road than we are.

Public safety has waited too long, and the American people have waited too long for the protection that they are entitled to, and for the protection that we are capable of giving them if we put our best efforts into it, and use the technologies and the know how, and the creativity that we have.

I know that you have got a lot to do. I watched this morning, and this is a long and arduous, but very productive, workshop thus far. My colleagues, I think all of whom were down here prior to me, look very much forward to your contributions.

We appreciate the time, and trouble, and sacrifice that you go to in order to be here, and as we move forward on our outage and our reliability dockets, we are going to rely heavily on your good advice and good counsel.

And finally I want to thank Chairman Genachowski for his leadership on these issues, and Admiral Barnett, and our excellent team -- Jeff and others -- in the Public Safety Bureau, for putting this workshop together, and thank them, too, for their vigilance during these past weeks have been so busy,

and we can probably count on some busy ones coming up, too.

So thanks for contributing to the work of the Commission, and the work of the country, and I appreciate the opportunity to come down and say that personally.

(Applause.)

MR. GOLDTHORP: Thanks, Commissioner. Could I ask our panel to come up and be seated now.

(Pause.)

MR. GOLDTHORP: As the day goes on, I am finding that I am leaving things all over the place. I already lost my glasses once, and my notes, twice. So, anyway, all is well now.

Thank you everybody for being here, and to our panelists for joining us today, and I am looking forward to the time that we have here. let me do this. Since a lot of these are folks that you have already met on other panels, I am going to through this myself, and just introduce everybody very quickly.

John Carlson, and you have already met him on the first panel. John is the Managing Director of Global Oversight for Morgan-Stanley. He is here today representing the Financial Services Sector

Coordinating Council.

Next to John is Robert Kondilas. Robert is -- I want to get your title right, Robert. Robert is a Cloud Strategist for the Computer Sciences Corporation. thank you for joining us today.

And next to Robert is Anthony Myers. Anthony is the Chairman of the Maryland Emergency Numbers Systems Board for the State of Maryland.

And next to Anthony is Scott Robohn. Scott is the Director for Technology and Solutions for the Americans for the Juniper Networks. Scott is here today representing TIA, the Telecommunications Industry Association.

And next to Scott is Mike Rowley, who you met earlier. Mike is the Interim Chief for Network Reliability for the New York State Department of Public Service. Thank you, Mike.

And then finally we have Duminda Wijesekera. Duminda is an Associate Professor in the Department of Computer Science at George Mason University. So, again, we appreciate all of you for being here.

This third panel is going to cover a range of topics that is very different from what we talked about in the first panel. In the first panel, we talked about outage reporting.

The subjects that we talked about there were all topics in a notice of proposed rule making, where we have proposed rules, and we have come to conclusions.

So we are further along in the process. The things that we will be talking about now are subject to a notice of inquiry that was released by the Commission in April, and the topics covered in that notice of inquiry were communications maintainability and resiliency when presented with sort of traumatic events, like hurricanes, disaster events that affect communications, and how quickly do they respond, and how well do they hold up.

That is one topic of that notice of inquiry, and a second topic is broadband reliability, and the nature of an NOI is altogether different. The questions that are asked are much more open-ended and broad.

There is no tentative conclusions, and no proposed rules. We do an NOI typically -- and in this case it certainly is true -- in areas where we have a lot of uncertainty about what we should do, if anything.

It may be that in some of these areas that we shouldn't be doing anything, and in other areas,

maybe we should be doing something. So it is a much more open-ended process.

So we would like to explore those kinds of topics with you today, and I would like to do it in three categories. This is all very timely, and you have heard this a number of times already today because of past events; the earthquake that we had a few weeks ago, and the recent hurricane, which we have become more accustomed to in recent years.

And these have reminded us of the kinds of things that can happen in communications networks when things like that occur. So let's talk about what happened after the earthquake first.

If you lived in this area, what you probably noticed was that it was very difficult to complete a cell phone call. You may have noticed that it was hard to complete a call on a wireline network, but that was less likely.

And so it has caused us to wonder about what if anything should be done to make commercial communications networks, particularly wireless networks, more resilient when confronted with surge events like that, and what are some of the techniques that could be used.

But let's drill down first, because that is

a big question. There are certain types of communications that are more important than others. So that is just my personal views. So, maybe 911 calls are more important than other types of calls.

Are there ways in commercial networks, wireless, wireline networks, today to -- since a lot of the congestion that was happening was happening very close to the edge of the network, and maybe the radio access network, for example, are there ways to detect when a 911 call is being presented to the network, and then to give it, to grant it, some form of priority that would make it more likely the call would be completed to the PSAP.

That is question that I will just open up and ask what folks think about that, and if it would be good policy to do it, in addition to whether it is technically possible. Does anybody have any ideas about that?

MR. KONDILAS: Jeff, I think that would be a good idea. I mean, we do this in a certain capacity with respect to ISP communications today. So the only challenge that I see is that if you have a central office that has so many circuits that can accept a call that if everybody is making a call, it won't get the 911 call.

If there is a thousand circuits, the thousand-and-first call that comes into the que won't get serviced, and there is no way to service the call. So then you have to get into resource reservation, which means that you have headroom, and if the central office can handle a thousand simultaneous calls, then you determine that five percent will always be available for 911, then you are going to have to have 50 circuits that are sitting and waiting, and not being used.

So what you are doing is that you are taxing the people that are trying to make calls for communications, which may be important, but are not 911 calls.

MR. GOLDTHORP: And let me remind everybody -- and that was fine by the way, but I just want to remind everybody to speak close to the microphone when you speak, okay?

It is about four fingers away if you can remember that, okay? And that was just right. I think that came through fine. Go ahead, Mike.

MR. ROWLEY: I can certainly attest to the previous statements. A lot of what we are encountering now with the Irene restoration is the need for back haul, and the importance, and the

reliance of cellular communications on the back haul networks, which are still mostly traditional telephone.

You have got to make sure that that is still running, and you have got to make sure that is resilient. I am sure that we are going to get into backup powering and diversity, but the more wireless that you put in, the more wires that you put in, and that is what we are finding.

MR. GOLDTHORP: You make a good point. I am going to cover these things, and I am going to get into those very issues of communications network resiliency and restorability when presented with a situation like that, and also broadband reliability

I am wondering though, you were talking about the need to do resource reservation, and to do what I was describing, but in an IP environment, were you thinking of things in terms of sort of an IP environment, or were you thinking in terms of a Legacy environment when you said that?

MR. KONDILAS: Well, I think about in both respects. I think that in a Legacy environment that it is more of a physical reservation that you are making, but in an IP environment, you still have a resource reservation that maybe is more virtual,

because it is packet based, as opposed to circuit based, or circuit switched.

MR. MYERS: I was just going to say that maybe to start, that I am here as the Chairman of the Maryland Emergency Numbers Systems Board, but I am also an Assistant Executive Director at the Maryland Public Service Commission.

So the combination of those positions allows me to look at the delivery of critical services, particularly 911, from a fiscal operation, but also regulatory perspective.

And public expectation is that critical services -- 911 calls -- will get through, and I think that we have to start from that ultimate goal, and almost reverse engineer the process to determine what types of standards, conditions, metrics, or other policies, are necessary to achieve that ultimate goal.

But that is where I think the conversation begins, with public expectation, because they don't understand -- the public today does not understand the distinction between legacy networks, which are buttressed on decades of State, local, and Federal regulation. And so that is what I would add.

MR. GOLDTHORP: Thank you.

MR. ROBOHN: To Anthony's point, there is

not only the very high bar that has been set through a regulatory framework for the public switch telephone network, but there is also being able to be a competitive service provider.

And I think that we heard some comments in the previous panel that the network doesn't really provide value even in non-emergency situations, unless it provides connectivity almost all the time.

So there is a tremendous amount of engineering, architecture, and implementation of redundancy mechanisms to keep the network up. In over subscription events, there could be more than just an emergency situation.

MR. GOLDTHORP: Duminda.

MR. WIJESEKERA: Yes, to get back into the reservation. I do agree that there has to be a certain amount of reservation, band width, and so on, set aside. But the thing is that there are two sides.

One, even if you do that, you could still run over the capacity, and this has been an issue in the DoD arena, and that is why they have not only reservation, but also preemption; a call that is considered more important can cut off a call that is not important.

They do it for different reasons, too, but

you could try to get some sort of preemption as well which may not be a good thing, because then you would have some unsatisfied customers if they are dropped in the middle of a cell phone call.

The second thing is that there are certain virtual techniques, which like I think you mentioned MPLS and so on. You could make some sort of virtual reservations with circuits that would among other things preserve the QoS, because it reserves capacity on the intermediate routers, and so on, and so forth.

So there are some techniques, but the question is that nothing comes free. You have two or three phases of negotiation and reservation, and that takes time, and that takes packets.

They need to be communicated in time and so on. So it is a balancing act I would say at the level of the protocol, and the algorithms.

MR. CARLSON: And I would add that maybe you were getting to this in your next scenario beyond the earthquakes, but some of the exercises that we had done several years ago looking at the impact of a pandemic, an H-1/N-1, in terms of the shift of how people would work, or be at home, as opposed to being in their offices, and not in schools, and a lot of broadband applications.

And from those exercises, we recognized -- at least for our sector, that we would have pretty significant issues with respect to internet congestion, particularly at the last mile level.

And so that let to a lot of discussion around, and well, what should the policy be around you setting priorities, and then how do you determine what is a more critical activity that should get priority service.

And that kind of led us to a discussion around, well, we should probably set priorities for those that are part of the critical infrastructure, or health and safety related issues.

Obviously, emergency 911 would fit in that category, but I don think that there needs to be a broader discussion around when you have capacity limitations in emergency situations, how do you shift into a prioritization regime.

And it is complicated, and a lot of unsatisfied customers, and a lot of people will disagree as to what is the priority, but that discussion still needs to be had.

MR. GOLDTHORP: I can remember the last -- not the current CSRIC, but the last CSRIC. We had a working group, and a report voted out on this very

issue of Next Generation priority service, and almost like a Next Generation WPS for IP based services.

And I don't know if it was dealing with the policy decisions or recommendations, rather, about what should receive priority, but it certainly has been a active area of interest here at the Commission.

And one of the things that we would need to be thinking about is what should we do next. What is needed for -- I mean, how should we engage in that discussion, and where is it.

And I kind of like the fact that we are talking more about -- and on this topic about broadband services. I wonder if -- well, let's just talk about wireless for a second.

And I wonder whether 4-G wireless technologies have the hooks baked into the protocols that would make it a lot easier to do the kind of resource reservation that would be necessary to do priority services, like what we are describing.

And since it is so early in the deployment of that technology relatively speaking, whether or not the features that we are talking about could be rolled out as part of the first generation, or near first generation deployments of 4G technology. Has that ever occurred to anybody?

MR. ROBOHN: Well, I think that there are a couple of interestingly related factors to that. Many 4G deployments today actually have multiple radios in them; a 4G radio for data, and a 3G radio for voice calls.

And to bring it back to the earthquake scenario, I remember very clearly that I was forced to get outside of my building, and I tried to make a call, and couldn't make the call. That was a 3G issue.

But I just instinctively went to Twitter to see what was going on, and was this really an earthquake. And the 4G service was still up. But there is a little bit of diversity built into a handset for a provider that is rolling out 4G in that way.

MR. KONDILAS: I think the underpinning of 4G is IP, and so it is easier for you to apply a priority of service to IP than it is to voice service.

MR. ROBOHN: But you still have issues there because you don't know if it is IP if the RAM is congested. There is an issue before that first terrestrial hop.

MR. GOLDTHORP: but if you can do -- I thought with 4G, with LTE, for example, that you could

do prioritization in the RAM, so that you would not run into the problem that we ran into during the earthquake, where in many cases the RAM got congested.

And if these things were running 4G, even for voice calls, you would be able to allocate capacity on a priority basis if things were configured that way.

MR. ROBOHN: I would have to go back and take a look. I know that YMAX, a competing 4G technology, had that built in, but I don't recall if LTE has that built in.

Then there is the issue of even though the capability is there, is the operator making use of the capability.

MR. ROWLEY: Yes, I was kind of trying to get to that in the previous question, at least for voice anyway, that you have got to make sure that the capacity exists where you hand off the voice.

And then at the back end are the emergency responders or whoever is expecting to receive the call, do they have the proper capacity. And that is sometimes a challenge in these emergency events.

MR. GOLDTHORP: Let's see. Let me do one more question on this topic, and then we will change to the next topic. That is a really good point that

you raised, which is that it is one thing to open up the network wide so that all of the 911 calls get through.

It is another thing to have the PSAP community configured in a way where they can actually absorb all of those calls. I mean, they are staffed at a certain level. They may not want to be getting all these calls, right?

And sometimes those calls are just things like was that an earthquake that I just felt. I mean, they are not emergencies sometimes, or they are copycat calls so to speak.

So I guess a question that has been on my mind is that even the Chairman today talked about NG 9-1-1, and how we are going to be moving forward in September, or I think it is this month, with NG 9-1-1. You know, with something on NG 9-1-1. I am pretty sure it is this month.

Now, with NG 9-1-1, does that now give you the level of flexibility in terms of dynamically allocating calls to a number of PSAPs that didn't exist in today's more restrictive environment.

So that the calls could be routed to a PSAP that is equipped or staffed to handle them. Is that a realistic scenario, and I know -- well, is Roger still

here?

Well, Roger Hixson and I talked about this earlier, but why don't we see what the panel has to say about this, and then I am going to ask Roger if he has got anything to add. Go ahead, sir.

MR. MYERS: Absolutely, part of the added functionality that NG 9-1-1 will provide will be additional flexibility in routing, and call assignment, and so forth.

To touch on a point that you made at the outset of the question regarding PSAPs, I just want to say that absolutely, even in an overload situation, PSAPs absolutely want to receive calls, because there are factors and procedures that the entities can put in place to mitigate the problem.

For example, PSAPs can put out public pronouncements to have persons who have true emergencies to go to a local fire station, or a local police station, or to take any one of a number of measures that may not solve the problem, but certainly lessen its impact.

MR. GOLDTHORP: All right. Yes, that is a good point. So you can kind of manage the flow by doing things from the PSAP out. Does anybody else have anything that they want to add on NG 9-1-1, and

how that can play into this?

Roger, you have been doing a lot of work on NG 9-1-1, and why don't you -- is there a way to activate -- yes, you can use the podium, Roger.

MR. HIXSON: Yes. NG 9-1-1 is my life. My wife would certainly agree with that. And to reinforce what you said, NG 9-1-1's design in the NENEF image of it provides for what we call dynamic routing, among a selected number of PSAPs, pre-established, or even in some cases, you would be able to dynamically change that process, too, because in today's E 9-1-1 world, you basically have fixed alternate routing.

If a PSAP has five trunks and all five trucks are full, and note that they might not actually be emergency calls, the next call would roll over to an adjacent PSAP as defined by that set of PSAPs as to how they want that to work.

And the second one might roll over to another one, but NG 9-1-1 is designed so that you can select a grouping of PSAPs that will back each other up essentially, and that can be automatically done on the fly without any specific action at the time that the calls are happening.

And in addition to that, there is a policy

routing function in the design of NG 9-1-1 that allows PSAP managers to go in by terminal and modify those arrangements, as compared to the old manner in today's world, where you basically have to call the telephone company, and you have to find a translations guy who knows how to do that.

And of course three of the four translations guys who knew how to do that left the company last week, and so it becomes difficult to get that accomplished and time consuming.

But NG 9-1-1 itself will do that automatically if you will within the system design.

MR. GOLDTHORP: Thanks, Roger.

MR. HIXSON: Oh, I forgot to mention. Duront used that same type of capability during the Hurricane a week or so ago, in which they had, I think, seven PSAPS who were backing each other up, and so they have already got a version of that in place, and it worked for them quite well from what they had to say about it.

MR. GOLDTHORP: So, there is hope on the network side, and there is ways to do on the PSAP side to deal with the flow of calls, assuming that we can find a way for the network to get the calls through.

And so the issue right now is more at the

originating side on the network, and in this case, we have been talking about the remote access, or the radio access network.

So, okay, that was helpful, and I am going to switch to another topic now, which is more general, disaster response and the resilience of communications during and after disasters.

And the questions in the notice that are pertinent to these topics were questions that originally came to our minds after Hurricane Katrina, and we actually had a proceeding about this.

One of the recommendations that came out of, or one of the actions that came out of the proceedings was a set of rules on backup power, and specific to network elements that required power, and how much backup power they should have available to them.

And those rules are not in effect right now. They were challenged, and they are not in effect, but we thought that it was time to revisit these questions, but in a broader light.

So when we asked the questions in the NOI, we didn't ask questions specifically about backup power, although there are questions about backup power in there. But we were asking questions in a much broader sense, because there is a lot more than just

backup power at stake here.

There is back haul, and I think that we have already talked a little bit about that. I think, Mike, you mentioned back haul. It turns out that when you have got something -- and in the last storm, we had most of the outages that we saw in the local access network were back haul related, and not backup power related.

That was a surprise to me, but not to John, and I don't know why. So it is not all backup power. Some of it is back haul. Some of it is just having crews getting access to the equipment so that the batteries can be backed up, and where the generators can be refueled, and so there are accessibility issues, and so there is a whole range of issues.

And then there is another issue on top of that, which something like this happens, and when we had Irene blow through, the counties that were the most affected, and suffered the most damage, were evacuated.

And those evacuations were lifted at some point, and folks started coming back. I don't know whether communications were completely restored, but there is that factor.

So we are asking questions now that are much

more holistic, in terms of what -- first of all, what do communications providers do to prepare for catastrophic events like this. What should they do.

And what do they do to restore services as quickly as possible, and then that leads to the question should the Commission be doing something to try and close any gaps that exist between things are done today, and how they should be done.

That is the long and the short of the question. Now, I didn't get into all of the details, but I am wondering if folks have any views on those kinds of issues. Mike.

MR. ROWLEY: Certainly we deal more with the physical redundancy and resiliency characteristics. We are aware of the dynamic routing that is available in IP, and that often leads to less outages, and less frequent outages, but a lot of times they are sometimes more severe.

So maybe that is for the other question, but I mean that I still think there needs to be some level of basic requirements for redundancy, and of critical circuits, and backup powering.

I think that what we have seen in the last couple of storms, a lot of the network providers are doing that on their own. There is a lot of

development of best practices that is driving that, and we certainly appreciate that.

There are other things. I was talking to John earlier about what we looked after 911 for the business community in New York. There are other non-physical things that you can do, such as we instituted critical facilities administration, where Enterprise customers can go and actually look, and go to their carrier, and actually have them physically map out where their connections are going.

So at least it gives that purchaser and end-user of the service some confidence in where their circuits are going, and to me, reliability is nothing more than a confidence that your network is going to work.

You know, the physical stuff is more about the resiliency, but you need that confidence in your network, and the services that you are purchasing from.

MR. MYERS: I would add that from my perspective that adequate redundancy, backup power, fault power, they are obviously integral parts of the Legacy network, and I think that it goes without saying that they are necessary components of any future for broadband network.

To say it differently, those are simply the price of admission. In Maryland, some of the things that we have done to promote reliability is that we ensure that -- well, we have 24 PSAPs, and approximately 900 call takers around the State, and we generate -- our citizens generate about 5.2 million 911 calls per year.

Each of our PSAPs has a dedicated backup facility that is geographically diverse. It is supported by generator and UPS, a power backup. We have worked collaboratively with Arlet, who is Verizon, to drive facility and route diversity, and to identify and eliminate single points of failure. So those are some of the things that we are doing.

MR. KONDILAS: I think what we have to do is look at -- there is a level of redundancy, and there are associated costs with that, and for carriers and all interested parties, that does come down to -- it is a dollars and cents discussion that happens.

You can achieve reliability and redundancy where nothing ever breaks, but it is at a certain cost. But I think what you have to do is create a graduated scale as to the constituency that is being served, and you can look at it from multiple different ways.

You can say the financial district in downtown New York may have a need, or it could be the number of people that are served in a certain area, and that you have to create redundancy in order to complete calls, or complete data transmission to serve in a reduced fashion, but still be able to do it for a certain subset. But it all comes down to costs, I think.

MR. GOLDTHORP: So the -- well, before I go on, does anybody have anything? John, did you want to say something?

MR. CARLSON: I would kind of echo what Anthony said about the cost of doing business, and I think that there is also a recognition that in particular the telecommunications industry, and in all of its variations, is becoming more and more integral to our lives.

I mean, we are using it more and more to do our business, and for personal, and for public safety, and that has to be built in to the Next Generation products that are put forth.

I think there is also another thing that we certainly learned from a lot of the different exercises that the financial sector has had with the telecom industry is that there needs to be this cross-

communication, in terms of what the capabilities are so that there is transparency.

So that it matches up with what a financial institution's business continuity plan is, and so that it is linked to your power backup capabilities and plans.

And it is like peeling the onion. I mean, actually through each of these different events, new things, new vulnerabilities that you need to mitigate, and it just this discipline in which you have to constantly move forward and mitigate those risks, and work with your partners to solve them.

So, 9/11 for us was a huge wakeup call, and then we have had multiple other incidences, including the last three weeks, that further emphasized that we are going to have different types of events.

We have not had the pandemic yet, and hopefully we won't, but that is another event that we are going to have to really deal with, and make sure that we have redundancy built into the system.

MR. ROBOHN: I will just pile on this whole thread here. Anthony, I think you made the comment table stakes. This is the entry price, and I think that most providers would definitely agree, that if the network is not available, you are not going to

survive long in the market.

I can say from the equipment provider perspective, we can't sell to service providers unless we have multiple redundancy mechanisms within the network elements that we sell, and in our processes for upgrading software to make changes without interrupting service in the network.

There is a point where the costs to achieve that next additional bit of availability doesn't really pay off, and I know that there are some service provider folks in the audience. Maybe they will offer comments later. But you really need to hear their view, I think, to get a full picture.

MR. GOLDTHORP: I think it is a good point, and one of the things that we tried to do in the notice is to ask questions that were broad enough that the answer could be as far as what the Commission should do.

I mean, maybe the role for the Commission in this space is just to require that there be some transparency about what the carrier's plans are for dealing with the prices.

But what I am doing is that I am trying to -- well, that is a question, and I am wondering what you all think. I mean, it sounded like a lot of folks

thought that there was a need for some level of resiliency and reliability that could be depended upon.

And some agreement that there is a level beyond which the incremental gain and resiliency is probably not worth the incremental costs. So is there a need for the FCC to have a role in determining where that threshold is, and then to have some procedure for ensuring that it is being met? What do you think of that? Duminda.

MR. WIJESEKERA: Yes, perhaps come up with a description of failures, or multiple failures that could be tolerated by the different providers to that you could see that in combination what is the maximum number of failures, or kinds of failures, that could be simultaneously addressed, and still maintaining the necessary communication and infrastructure.

MR. GOLDTHORP: I think, Mike, did you want to say something?

MR. ROWLEY: Well, I didn't want to interrupt too many times, but in New York -- well, I guess my point is that there are lessons to be learned from what we have done in the Legacy networks, although I don't appreciate that word too much.

But after 9/11, we did a complete review of

the telecom resiliency and redundancies in the telephone networks. I know that we worked closely with Kevin Green and Verizon, and he can attest to it.

And what we did is that we set a baseline requirement similar to your costs of doing business. What would it cost for full redundancy of every office, and the necessary equipment, and then we took a step back and said, well, yes, that is how much it is going to cost for a hundred percent of the network.

But then we applied a needs based approach, and we found for a drastically reduced amount of money that we could get 97 percent of the network to meet those redundancy requirements.

And to us it was a cost based solution that we were very -- that we very quickly implemented, and we continue to monitor.

MR. GOLDTHORP: How did you accomplish that?

MR. ROWLEY: We had the companies do assessments, and go out and tell us, and report back in a year how you meet these requirements, and what are they going to cost to implement them.

MR. KONDILAS: I think that there is a role for the FCC here. I have seen in the past the government collaborate with industry in solving problems.

One of recent memory is the digital wire tap initiative -- you know, Colleah, where the government wanted the ability to do wire taps, and they worked with communications providers, or service providers, and equipment vendors, in order to build this initiative in.

And they did it in collaboration, and it had to be done by a certain date, and there was an inventive there for the service providers, and for the vendors to get that capability in place prior to that date, and there was also a penalty associated if it was not in place by that date.

MR. MYERS: I would add that certainly there is a role for the FCC. Part of that role is a recognition of the importance of State and local participation, and I think it is critical given the transition to a broadband network, which is not regulated by State and local authorities.

Many of the problems that can occur in the delivery of critical services will require a level of glandular review that can only be provided at the local level, and that glandular oversight will provide operational efficiencies that lead to the quick resolution of problems that occur.

In Maryland, the General Assembly

established the board that I sit on, and the use of 911 as an emergency number, or as the emergency number, and in recognition of the fact that avoidable delays occur at the jeopardy of threats to life and property of residents.

So with that in mind, the FCC has to be cognizant, or should be cognizant of the importance of that continued local participation.

MR. GOLDTHORP: I am going to move on now. There is a bunch of questions that I would like to ask about that topic, but I want to cover this last topic as well, and then we will either return to this, or we will take questions, depending on how many questions we have.

But let's now shift to the other topic area that was covered in the NOI, and I have described this to a lot of people, and I don't know if I still quite got it down.

Stacy, you and I have had this conversation two or three times now, and Scott, I had never talked to you about it, but it would be interesting to see how you react when I do this, because you are representing TIA, but I know that you are from Juniper. So I will be interested to see how you react.

It is an assertion, and I mean it that way truly. I am prepared to be challenged and told that I am wrong, but i want to know why I am wrong, and it's this. That years ago, and not too many years ago, we had this concept of carrier class networks.

There was a concept of five-nines reliability, and over the years, first as wireless services, and then broadband IP based services, have made their way into the communications networks.

And networks have become much more functional. That's true, but on the other hand, we have kind of in a way lost that concept of five-nines, or how to measure it, or even to know if it can even exist.

So I will give you an example. The globally routable internet was originally designed to be extremely resilient. You know, a full, tolerant network where things can happen in the network, and you can route around them.

And we have talked some about that already today, and the internet still operates on that principle. The networks that are being operated by sort of communications providers, carriers today using the internet protocol as a basis, are not the global internet.

I mean, they have gateways to the global internet, but when you route traffic around, it is not the internet, and you all know that. They are routing traffic around on MPLS, or some other higher protocol that enables them to achieve quality of service guarantees, and to route traffic efficiently in their networks.

But what it does is it takes what had been a connection list environment for networking, and sort of makes it not a connection oriented, but it adds a level of connection mist to the network that wasn't there before.

So now you have a sense of state. You know, it is a virtual circuit, or whatever the case may be. It is not a nailed up circuit. But now traffic in the network doesn't have as many degrees of freedom to move about.

And so that was the look that I was looking for. So you are the first person that I want to ask, and maybe you are the person that can answer this for me.

I am wondering if communications networks are more reliable today, or less reliable today, and given that we are relying on a connection list protocol, but we are running it in a connection

oriented fashion.

MR. ROBOHN: I will try to keep my response brief.

MR. GOLDTHORP: Does it make sense first of all?

MR. ROBOHN: Oh, yeah. So a couple of comments, and I am sure that other people will have things to add as well. So it is more complex. This is not your father's telephone network, right?.

It is a lot easier to measure five-nines for reliability when the only service is voice, and that is not an excuse for not measuring availability in Next Generation networks.

But now there is a much broader range of services. I want to get video over the internet, and I want to get voice over the internet. I get my e-mail over the internet.

So perhaps part of the alleged losing concept of five-nines availability has to do with that there is so much more to measure, and so many services are overlaying over the same network.

That is one reaction. I would say wearing my engineer and scientist hat, we have to look at the data. Again, I think part of the reason that we are having this discussion is maybe we don't have all the

apples to apples data that we want to compare Legacy network availability to today's network availability.

The last thing I will say, and then I will let go of the mike, I know that -- and again from my perspective in the food chain, I spent five years in Juniper's customer service organization, and it is not a fun job, because when there is an outage, and when you are a vendor that is in some way responsible for an outage in a service provider network, you are on the phone until it is fixed.

And again I am sorry to continue to beat the drum on this, but even on the side of emergency situations, service providers and their vendors have a vested interest in providing mechanisms to maintain availability of the network.

MR. GOLDTHORP: Okay. Thank you. Robert.

MR. KONDILAS: I would actually assert and reaffirm what Scott has said, but complexity is the enemy of reliability, and so the more and more services that you lay on top, the larger the network reaches.

And the reach is going from the handsets to people, and things like that, that you actually -- you have an issue of achieving five-nines of reliability, which we are used to.

But what I would assert is that while it has probably gotten tougher for us to get to five-nines, we understand more about how to get to five-nines, but I think that the constituency that is served is more tolerant of outages, because there are more avenues for them to communicate.

So the PSTN goes out, and as Scott said, hey, I couldn't get on the network, and so I went outside, and I got on Twitter. So there are other avenues to communicate, where an outage on the one network, and only have one network to communicate, is more catastrophic.

MR. GOLDTHORP: Yes, I can see that. I can see that. So, it takes -- you really would have to look at this in a whole new way to account for things like you are describing.

And things like not only is there a difference in services, different platforms. I mean, there is a multitude of different ways to communicate now that didn't exist before.

MR. KONDILAS: And accessibility is for the most part wireless. So it is not like that I can't use my phone, and I run over and get my cell phone. It is like everything is around me to use.

I am sitting at my computer, and I can do a

VoIP call over my computer. I can do it from my wireless phone. So it is ubiquitous almost in some respects.

MR. GOLDTHORP: What do others think? Does anybody else have an opinion about this? Mike.

MR. ROWLEY: I mean, just one observation, and I think it is getting at what you were asking. Today's network is so interconnected. I mean, we are talking strictly now about the IP network, but that network is so interconnected with the public network.

And each one of those interconnections is -- you know, there is dynamic routing, but there are single points of failures on other networks that are interconnected to that IP network.

And again I think that you have got to pay attention to that, and a lot of times what we find is that because there is so much hand-off of traffic, it is harder when there is an outage for the provider to troubleshoot it, and to report it.

And a lot of times, they may not know where the outage is occurring, but some farmer in Virginia hits a fiber line, and people in Buffalo can't talk. And that is the stuff that is important to us.

And again it is on the customer end, and what is the impact. You know, not necessarily what is

going on in the network, because we know that there is something going on, but we need to know how that is affecting customers at the end.

MR. GOLDTHORP: It is a good point that you make, and then I will ask others, but we have seen things like this, too, and not because we are getting any confidential data, but because they reported it in the press of something happening in the network, discreet happening in the network, in a carrier's network, and taking out service nationwide.

And that is a pretty big single point of failure, right? Or a single -- whatever it is, and I don't know if it is a point, or I don't know what all was involved, but from the sounds of it, it was close to that.

So it is that kind of thing, and is traffic being aggregated in a way that is uncertain, and what is the science. It used to be that there was actually a science behind the calculation of the reliability, and the probabilities, and so forth, that went into that.

You know, probability is probability, right? I mean, you are not at a hundred percent. You are at something like five-nines, which is pretty close. John, did we really ever have five-nines?

UNIDENTIFIED PERSON: With additional switches.

MR. GOLDTHORP: So it has happened, but anyway, but it could be calculated, and I guess I wonder is there any body of science that has come about to replace what we have known, and are there standards that are in development, or have been passed that can apply to try and bring industry along to get to that where industry should be. So should there be standards.

MR. MYERS: In a highly interconnected network, one can anticipate that the level of quality delivered will be equivalent to the level of service produced by the least reliable provider. Do you follow that?

Speaking empirically for a second, in terms of reliability of the network, in Maryland, we have experienced a series of outages recently that have impacted 911 operations, and the causes of those outages and impairments have been the result of everything from snow storms to signaling abnormalities, to human error.

And a lot of what we -- and how we responded to those outages, believe it or not, went back to just some good old fashion common sense; improving

communication amongst stakeholders, and we put in place a number of procedures that were instrumental in not only resolving the problem, but also prospectively avoiding the potential for the probability of those problems occurring again.

For example, we electronically and automatically disseminate vendor trouble tickets to our PSAPs so that they know when something is occurring among the networks.

We received a commitment from our Arlec to provide notice to our PSAPs within 15 minutes if their NOX discovers a facility outage, because often times what we experience during those outages as I mentioned is that a problem was occurring in a network that may not have appeared to the operator, or to the PSAP, nor did it readily appear to the NOX as to its potential impacts. So a simple improvement in basic communications has helped tremendously.

MR. GOLDTHORP: Thank you.

MR. CARLSON: I have only point to make, and that is because of the complexity, and in our sector the regulatory requirements to have robust business continuity plans, I think that a lot of financial institutions are over-investing in terms of their capabilities.

So we have expanded greatly the number of remote computing capabilities that we have. We have never reached the point where we have run into any problems, because we basically over-invested, and that's fine. We felt comfortable doing that.

I think that the other kind of issue related to the complexity and all the different applications, and I know that the telecom providers are just providing the pipes for the applications to go through.

But adding to that complexity is issues like malware that will impact not only networks, but also applications that are then running on the networks, and that has become another challenge.

And I think certainly our sector would like to see the ISPs play a greater role, in terms of monitoring the malware, and working in partnership with us in order to reduce the amount of malware in e-mail that is malicious in nature.

MR. GOLDTHORP: Thank you. Any other comments? I want to go now to open it up for questions from the audience, and ask if there is anybody here in the audience that has a question.

And if you do, please do as we have done before. Come up to one of the mikes here, and just

introduce yourself briefly.

MS. CANFIELD: Hi, I am Jill Canfield, and I am with the National Telecommunications Cooperative Association, and I think that these discussions are very important.

And my question kind of relates to the discussion that you just were having. We have a situation where calls are simply not completing to customers living in rural areas, plain old telephone voice calls.

The calls is not making it to the terminating carrier's network at all. We have situations where a school had an auto dial notification system, and calls didn't make it to parents, and so it was an emergency situation.

But this is not an outage, and it is am emergency, like an earthquake or tornado, or anything like that. But it is a persistent and continuous problem for customers living in rural areas.

And I guess my question is how do we ensure, and specifically, how does the FCC ensure that as we move forward that we cannot only ensure continued reliability, or I guess again ensure reliability of the telephone network that we all rely on and have continued to rely on?

MR. GOLDTHORP: Mike.

MR. ROWLEY: I can't talk to the solution to that, but I know that we have had that problem in New York, in rural areas of New York, and part of the problem is just intercarrier compensation, and carriers refusing to deliver traffic.

I know that they were addressing it here at the FCC, and even in some of the cases in the States, but that is part of the problem that we have when we have the IP carriers that are unregulated connected with the other carriers.

There is different compensation rates. I am hoping that is going to improve when we reform all of this, and it looks like that is being done. So hopefully that will improve.

MR. MYERS: I think one of the ways that you begin to address this issue is to not necessarily micromanage the operations of a company. I am certainly not a proponent of that, but to be reminded that as the industry evolves, enforcement remains an important component.

For example, in Maryland, the Public Service Commission has recently issued a show cause order to a vendor to show cause as to whether or not their services met the safe, reliable, and adequate delivery

as required by statutes.

And the Public Service Commission has fining authority of up to $10 thousand per violation per day, and some have argued that a violation can be on a per call basis. So that is perhaps one way of addressing the lack of continuity.

MR. GOLDTHORP: Okay. Thank you. I have a question that came in over the internet, and I am going to start with the last one that came in, because I can answer this one myself.

Annie from Maryland would like the FCC definition of connectionness. I kind of made that one up on the fly. So I will define it on the fly, too. Connectionness is the opposite of connectionless.

Okay. So I won't be flip about it. What I meant to say is as opposed to a pure connection list environment, which is a network environment that the internet was sort of born in, a connection oriented, or what I was calling a connectionness environment -- and a connection oriented environment is one in which individual sessions or calls have either virtual circuits or real circuits nailed up in the Legacy old networks, or networks that are still in use.

And calls were nailed up, and you had resources allocated for the duration of the session.

I am not talking about anything that quite static, but I a not talking about anything as dynamic as a pure connectionless environment, which is how the globally routable internet operates.

So that is how I would distinguish between the two, and maybe that term will make it into the term of art category. Okay. Is there any other questions in the room? I have some here, but if we have some in the room, I will go to one in here first. John. Well, we will do the FCC questions last, okay?

So this is a question, and I have not read these, and so there is no telling what you are going to get, okay? Anyway, this one -- I won't read the name of the person either, but it is from somebody from the Public Utility Commission of Oregon.

And this person is saying that our State carriers are telling us three days of backup power at COs, and eight hours of backup battery, and then all goes dead. An insufficient effort is what I think this person is saying, and is their opinion.

For a long term event, what are the plans and resources during a catastrophic event? FCC should establish measures and administered through State Commissions, with the Emergency Preparedness/Disaster Responsibilities.

And then Oregon PC is the ESF-2 and 12 liaison between utilities and CELEX, with the State of the Office of Emergency Management. Anthony, I think that this person probably shares a lot of what you were saying when we were talking on those kinds of topics.

It sounds like you are suggesting that an approach for this is for a closer collaboration between the Federal Government and what the States are doing. Am I right in reading that in?

MR. MYERS: I think that between or among the Federal Government, and States, and local governments as well.

MR. GOLDTHORP: You're right. That's true. So that is what I read into this, and so I don't see a question mark here. It seems more like a statement, and unless anybody wants to comment on what I just read.

MR. ROWLEY: Well, I will just add to Anthony, that one of the things that we look at following a restoration, and after the fact, and in an post-event analysis, is that we ask the carriers how did they comply with the NRIC, and now CSRIC best practices.

And they are not requirements certainly, and

we find most of the time that the carriers adopt those practices, and it goes a long way to keep the networks resilient.

MR. CARLSON: Well, at least in our sector, we do have regulatory requirements that are pretty stringent, and they are spelled out in terms of the need to recover within certain periods of time based on what type of institution you are, and what role you serve in the sector.

And the regulations have even gone so far as to say that you should have your backup sites in different regions, relying on different telecom, and different electrical utilities, and separate staff, so that you have true redundancy in various locations.

So that is one of our challenges, is making sure that we have plans that meet those requirements that are risk based, and that means that we really have to understand what the capabilities of the telecom providers, as well as others, like the power providers, in terms of their business continuity plans.

MR. GOLDTHORP: So, in answer to some of the questions that we were asked about communications survivability, it sounds like your approach has been much more risk-based, performance-based, and you

basically set requirements on how long -- well, what is the time frame for getting service restored.

MR. CARLSON: Correct.

MR. GOLDTHORP: So is that an approach that would apply to the communications sector?

MR. CARLSON: Parts of it could. You know, each customer is going to be a little bit different, and that is part of the challenge, is that our standards are typically higher than most of the customers that the telecom providers have.

So we are always kind of bumping up against this. Well, that's not commercial, and that is not what we are offering to our standard customer base, and you are going to have to pay more to have something that is more robust.

So that is an issue that we run up against, but it really starts with the risk assessment process, and looking at the business impact of any sort of number of events, and then building the plans around that.

MR. GOLDTHORP: All right. Thank you. And the last question that came in from the web, and this is from the same gentleman from Oregon, and he says again, or he says this time that telecom networks are less reliable as carriers claim less responsibility

for an outage because of multiple paths from origination to termination.

That again, I think, sounds like a statement, or an assertion, one or the other. I don't know if anybody wants to challenge that, but let's treat it as an assertion, okay?

Then does anybody have anything to say on that? How do people feel about that statement?

MR. MYERS: I think that there is some truth to -- there is potentially some truth to that, in that if you think about network topology in general, and the more complex it gets, the more access points, and the more participants, the probability for failure increases.

One thing to keep in mind as we think about Next Generation, or evolving networks, also is that we are going to have a different type of entity involved, and where we are transitioning from solely having carriers, or telecommunications carriers involved.

We are also going to have application providers involved. We are not regulated at the State level, and we are not regulated per se at the Federal level, and so it is going to be important to put in place contractually perhaps as the financial industry, the types of standards that we will require.

And we will probably also be faced with those entities, because entities will have different levels of experience, and different levels of resources.

We are also going to be faced with what do we do when those entities are no longer viable, or mid-contract, or before the expiration of a contract. I have been on the 911 Board for a number of years now, and there has not been anything more exciting or challenging than this proposition of moving to a broadband IP based network.

MR. ROBOHN: Can I offer a flip side of that? So a failure does not equal an outage. Let me tease that out. Yes, by definition, the larger a system is, with more discreet components, the higher the probability will be the failure of any one of those discreet components.

But there is network engineering practices where you put it together in the right way, you can actually build a more complex system to be more highly reliable.

It is not a linear connection of things. There is certainly other aspects that actually enter there, such as the interconnection points, and the other non-topological factors certainly come into play

here. But I wouldn't equate increased complexity with higher probability of an outage.

MR. GOLDTHORP: All right. Are there any other questions inside the room here? Okay. You are a hardy lot of folks for sticking it out.

(Pause.)

MR. GOLDTHORP: Okay. We just got a couple of -- well, okay, this is an easy one. This is the gentleman from Oregon thanking us for addressing his rhetorical assertions, and he says that Oregon Is pronounced Oregon. I guess I never knew that.

So I am going to just hold this one, because we are already a little bit over, and it has been kind of a long day for folks. So I appreciate everybody coming out for this, and for everybody staying for the whole event, and I especially appreciate the panelists for coming out and participating, and some of you doing double-duty, not only on this panel, but on the second panel as well, and the first panel.

So thanks everybody, and have a safe trip home, and we look forward to seeing you here again sometime soon. Have a good day.

(Applause.)

(Whereupon, at 3:06 p.m., the workshop in the above-entitled matter was concluded.)

REPORTER'S CERTIFICATE

WORKSHOP TITLE: Ensuring Broadband Reliability and Resiliency

WORKSHOP DATE: September 8, 2011

LOCATION: Washington, D.C.

I hereby certify that the proceedings and evidence are contained fully and accurately on the tapes and notes reported by me at the workshop in above entitled matter:

Date: September 8, 2011

Gabriel Gheorghiu
Official Reporter
Heritage Reporting Corporation
Suite 600
1220 L Street, N.W.
Washington, D.C. 20005-4018